CSS CYBER DEFENSE PROJECT

Hotspot Analysis:

Cyber and Information warfare in the Ukrainian conflict

Zürich, October 2018

Version 2

Risk and Resilience Team
Center for Security Studies (CSS), ETH Zürich

CSS ETH Zurich

ETH zürich

Author: Marie Baezner

Contact:
Center for Security Studies
Haldeneggsteig 4
ETH Zürich
CH-8092 Zürich
Switzerland
Tel.: +41-44-632 40 25
css@sipo.gess.ethz.ch
www.css.ethz.ch

Analysis prepared by: Center for Security Studies (CSS), ETH Zürich

ETH-CSS project management: Tim Prior, Head of the Risk and Resilience Research Group; Myriam Dunn Cavelty, Deputy Head for Research and Teaching; Andreas Wenger, Director of the CSS

Disclaimer: The opinions presented in this study exclusively reflect the authors' views.

Please cite as: Baezner, Marie (2018): Cyber and Information warfare in the Ukrainian conflict, Version 2, October 2018, Center for Security Studies (CSS), ETH Zürich.

Table of Contents

Executive Summary

Targets:	Ukrainian and Russian institutions, media outlets and connected devices.
Tools:	Distributed Denial of Service[1] (DDoS)[2], website defacement, malware (BlackEnergy, Snake, Operation Armageddon, X-Agent, CrashOverride, NotPetya, BadRabbit, VPNFilter, Python/Telebot), propaganda, and misinformation.
Effects:	Unavailability of targeted websites, information stolen from infected networks, electricity outage for several hours in Ukraine due to an attack on several power plants, damaged computers and devices propaganda and misinformation campaigns.
Timeframe:	November 2013 and still ongoing

Russian intrusion into American computer networks during the US election attracted significant attention in the West, and publicly demonstrated their cyber capabilities. Yet Russia has been developing and improving its cyber arsenal for the past ten years, as Russian cybertools have been in play in Estonia in 2007, and strategic cyberattacks were deployed during the Russo-Georgian war in 2008. During the Ukrainian conflict that started in 2014, Russia demonstrated its capacity to combine cyber capabilities with electronic warfare, intelligence and kinetic capabilities.

This Hotspot Analysis examines the specific case of the use of cybertools in the Ukrainian conflict. A “hotspot” is understood as the cyber-aspect of a particular conflict and relates to the series of actions taken in that context by states or non-state actors in cyberspace.

The main objective of this analysis is to better understand the events and cyber-activities that took place during the Ukrainian conflict and their effects. An additional aim of this document is to evaluate victims’ responses to the cyberattacks in order to learn from their reactions.

Description

At the end of 2013, the Ukrainian President abandoned an Association Agreement with the European Union that would have strengthened ties between the entities significantly, triggering mass public demonstrations. A few months later, disgraced President Yanukovych fled to Russia, and Russia invaded the Crimean Peninsula. Throughout the Euromaidan protests and the resulting conflict, institutions and media outlets in both Ukraine and Russia fell victim to DDoS attacks, website defacement and Remote Administration Tools (RAT) delivered by spear phishing emails. These cyberattacks were used to either disrupt, spy on or damage the enemy. By employing non-state actors as proxy forces to conduct these attacks, the warring parties were also ensured of plausible deniability for their actions in cyberspace.

Effects

The analysis found that the cyber-activities conducted in the context of the Ukrainian conflict not only affected Ukraine at the domestic level, but also had repercussions internationally. The social and political effects of the cyber-conflict in Ukraine included the domination of Crimean news and information sources by Russia, the erosion of Ukrainian government’s credibility among Ukrainians, and a loss of trust in the government for the Ukrainian population as a result. Economic effects included the costs of the loss revenue and reputational damage caused by the various DDoS attacks and website defacements and the expenses incurred by the need to replace equipment following cyberattacks on the Ukrainian power grid. Technological effects comprise the risks of heavy dependence on foreign technology, having enemy troops physically tamper with telecommunications infrastructure, the ramifications of cyberattacks on the Ukrainian power grid, and the development of new malware.

At the international level, cyberattacks in the Ukrainian conflict exhibit a low-intensity tit-for-tat logic between the warring parties in cyberspace. Additionally, while Ukraine experienced limited support from the international community, significant economic sanctions were instituted against Russia.

Policy Consequences

A range of policy consequences can be derived from the effects of cyber-activities that occurred in the Ukrainian conflict and in the Russian information warfare campaign. As in, proactively try to bolster their own situation so their state does not fall victim to propaganda campaigns in the same way that Ukraine did. Additionally, states should enhance the cybersecurity of online state infrastructures against Distributed Denial of Service attacks and website defacement. In addition, nation states may wish to improve their cybersecurity by limiting their dependency on foreign technology and providing guidance for the private sector on how to respond following a cyberattack. States should closely monitor how the Ukrainian conflict continues to evolve, and

[1] Technical terms are explained in a glossary in section 7 at the end of the document.

[2] Abbreviations are listed in section 8 at the end of the document.

promote Confidence Building Measures at the international level.

Addendum

This is the second version of the Hotspot Analysis on Ukraine, and includes an addendum at the end of the document. The addendum covers the period from January 2017 to June 2018 and its purpose is to update the earlier version of the Hotspot Analysis and provide additional information on the events that occurred in advance of and during that period of time. Those six months saw new malware that targeted Ukrainian networks, and two reports were published that brought new information to light regarding the cyberattack on Ukraine's electrical grid in 2016.

The addendum is structured like the main Hotspot Analysis to keep consistency between the two versions of the report. The addendum only reports new elements in the case of Ukraine and seeks to avoid repetition with the main Hotspot Analysis. Therefore, the addendum cannot be read on its own and should be read in addition to the original Hotspot Analysis. In addition, Appendix 1 from the earlier Hotspot Analysis has been incorporated into the addendum and includes new elements. The addendum is organized as follows. In Section 2, it first details a chronology of the events that occurred between January 2017 and June 2018. Section 3 examines the malware that targeted Ukraine during that period. This section focuses on the malware CrashOverride, NotPetya, BadRabbit, Python/Telebot and VPNFilter. This section also gives more details on two pro-Russian hacker groups: Sandworm (previously called Quedagh), which is a subunit of APT28, an actor that was examined in the main Hotspot Analysis; and the Gamaredon Group, which the main Hotspot Analysis attributed with Operation Armageddon. Section 4 analyzes the effects of these attacks on Ukraine and its international relations. It first examines the social and political effects of the cyberattacks. It shows that since the beginning of the conflict, Ukraine has developed its cyber capabilities and is increasingly aware of Russia's online influence campaigns. As such, Ukraine has begun attempting to limit their effects. However, a feeling of insecurity remains in the Ukrainian population due to recurring cyberattacks. The cyber-campaign against Ukraine had significant economic effects on Ukraine, including the consequences of ransomware attacks and the replacement of technology due to cyberattacks on the electrical grid. Technologically, the Ukrainian conflict revealed new sophisticated malware, some of which imitating known malware to confuse observers. Additionally, Ukraine has most likely become a testing ground for the further advancement of Russian malware. Internationally, the situation in Ukraine indicated that even though cyberattacks in Ukraine were sophisticated and were increasing in intensity, attacks remained below a certain threshold that would trigger an international intervention. This fact also emphasizes the lack of international support to Ukraine in its fight against pro-Russian separatists and cyberattacks. Section 5 gives some general policy recommendations to help states avoid a similar situation as in Ukraine.

1 Introduction

Over the past ten years, Russia has repeatedly shown that it is capable of developing its cyber capabilities and effectively integrating them with its other military capabilities (e.g. kinetic, intelligence and electronic warfare (EW)[3]). Perhaps the earliest example was from 2007, with the use of Distributed Denial of Service (DDoS)[4] against Estonian government institution websites. By 2008, during the conflict between Russia and Georgia, Russian capabilities had improved to the extent that cybertools were successfully combined with kinetic forces. This Hotspot Analysis examines specific cases in the context of the Ukrainian conflict to better understand actors' dynamics and modus operandi in this region. The goal of this report is to analyze how victims, both individual and institutional, were affected by cyberattacks and how they responded. This paper also serves as a basis for a broader comparative study of various Hotspots that can be used to inform other states on how to improve their responses, if faced with similar situations.

This Hotspot Analysis report will be regularly updated as new details are released or important events occur. The aim is to keep the document as up-to-date as possible.

This report analyzes the specific case of cyber-activities in the Ukrainian conflict. Relations between Ukraine and Russia have been tense ever since Vladimir Putin was first elected president of Russia in 2000. Their strained relationship was punctuated by disputes in 2004 during the Orange Revolution in Ukraine, and again regularly over natural gas supplies. Tensions reached new heights when Ukraine began developing closer relationships with the European Union (EU) and Ukraine's Russia-friendly president Viktor Yanukovych was ousted following the Euromaidan protests. The two nations finally erupted into an open conflict when Russia invaded the Crimean Peninsula.

This case warrants close examination because it concerns an ongoing conflict that is characterized by an intense cyber-dimension. While the intensity of the conflict has decreased in both the physical and the cyber realms, it remains a significant factor in world politics and may influence events elsewhere, for example in Syria where Russian troops are also deployed.

This Hotspot Analysis is divided into the following five sections: Section 2 describes the historical background and chronology of the events from Ukrainian independence in 1990 to the renewed violence in the Donbass region in January 2017. It records the events that have most influenced the tense relationship between Russia and Ukraine, and situates the cyberattacks in relation to the broader context of the conflict .

In section 3, the report explains the various cybertools and techniques used during the Euromaidan protests and the Ukrainian conflict, as well as the various targets and perpetrators. It demonstrates that the tools and techniques used in this conflict display different degrees of sophistication and serve different purposes. The reported cyberattacks included DDoS; website defacement, which was mainly aimed at disrupting proper website function; – and several malware families that were used to steal information. The victims of cyberattacks were mostly state institutions and media outlets in both Ukraine and Russia, but also Ukrainian armed forces and third parties (e.g. international organizations and other states). The perpetrators are categorized into two groups based on their affiliations. Therefore, actors are either classified as a pro-Ukrainian hacker group, or a pro-Russian hacker group. Both Ukraine and Russia conduct cyberattacks through proxies, which enables both governments to deny any direct involvement.

Section 4 examines the diverse effects of the cyber-aspects of the Ukrainian conflict on the domestic and international level. On the domestic level in Ukraine, the effects were felt in the social, political, economic and technological domains. Sociopolitical effects in Ukraine included a denial of access to non-Russian information on the Crimean Peninsula, and a loss in trust in Ukrainian institutions' ability to protect society. The economic costs of cyber warfare included the costs of loss revenue and reputational damage caused by DDoS attacks and website defacements, as well as the costs of replacing damaged equipment in the power plant that was targeted by a Russian cyberattack. Technological effects consist of Russian troops physically tampering with telecommunications infrastructures in Ukraine – an aspect that clearly illustrates the dangers of relying on foreign technology; of the physical damage to technological equipment in power plants due to the cyberattacks; and the discovery of new malware. Effects on the international level can be characterized as low-intensity, and the warring parties were seen to employ a tit-for-tat logic even when critical infrastructure such as power plants were targeted. Additionally, the limited support that Ukraine received from the international community has major global implications, as does the implementation of economic sanctions against Russia.

Finally, section 5 proposes some conclusions that may be drawn from this Hotspot Analysis and that state actors can learn from to reduce the risk of being impacted by cyber-activities resulting from the Ukrainian conflict or to avoid a similar situation. It suggests improving cybersecurity by raising public awareness of the issues of propaganda and

[3] Abbreviations are listed in section 8 at the end of the document.

[4] Technical terms are explained in a glossary in section 7 at the end of the document.

misinformation; leading by example with better protection of online state infrastructures against DDoS and website defacement; and limiting dependency on foreign technology. It also recommends closely monitoring the development of the Ukrainian conflict and promoting Confidence Building Measures (CBM) in cyberspace to reduce mistrust among states, but particularly Ukraine and Russia.

The addendum shares the same structure as the main Hotspot Analysis. Section 2 outlines a chronology of events in Ukraine between January 2017 and June 2018. Section 3 describes the new malware observed during that period in Ukraine and provides new information on actors present in the Ukrainian theater. Section 4 analyzes the effects of the additional cyberattacks on Ukraine and on international relations. Finally, Section 5 gives some general recommendations states can use to ward off similar cyberattacks as the ones in Ukraine.

2 Background and chronology

Both the historical background and chronology of the Ukrainian conflict are important in understanding the context in which it developed.

Ukraine gained its independence at the fall of the Soviet Union, but Russia still tried to maintain a certain control or influence over former Soviet Republics. The relations between Russia and Ukraine have been characterized by disputes, including the Orange Revolution during the Ukrainian elections in 2004 and disputes over natural gas supplies. Ukraine first initiated its rapprochement with the EU with an association agreement, but later turned back towards Russia instead. This decision precipitated the Euromaidan protests and provoked the departure of Ukrainian President Yanukovych. In parallel with the protests, DDoS and website defacement occurred on Ukrainian websites. A few months later, when Russia invaded Crimea, there was another increase in cyber-activities in Ukraine and Russia, but these then dropped again to a more or less constant low level. However, there were two spikes in the form of two attacks against the Ukrainian power grid.

Rows with gray background refer to cyber-related incidents.

Date	Event
05.12.1994	Ukraine becomes a member of the Nuclear Non-Proliferation Treaty by returning its nuclear weapons to Russia. In the Budapest memorandum on Security Assurances, Ukraine is assured that its territorial integrity and political independence would not be threatened by Russia (Besemeres, 2014; United Nations, 1994).
03.2005-01.2006	In March 2005, Russia accuses Ukraine of diverting natural gas bound for EU states and not paying taxes on natural gas supplies. On January 1, 2006, Russia cuts off natural gas supplies to Ukraine, with effects on European states that depend on the gas supply transiting through Ukraine (BBC News, 2006).
08.2008	Russia invades Georgia following skirmishes between pro-Russian rebels and Georgian armed forces. The Russian military uses a combination of kinetic capabilities and cyberattacks on Georgian institutions' websites (Giles, 2016a, pp. 4–5).
12.2011	After Putin's victory in the legislative elections, the opposition organizes demonstrations to protest against the election results. During the protests, the Russian armed forces use automated DDoS to disrupt media and social media pages in order to stop discussions of the elections (Giles, 2012).
11.2013	The Ukrainian President Yanukovych rejects the Association Agreement with the EU. The pro-European Euromaidan movement subsequently organizes protests but is violently repressed. At the same time, Ukrainian institutions' websites are targeted by DDoS attacks[5] (Ukraine investigations, 2014).
18-21.02.2014	Violence against protesters intensifies causing the deaths of several demonstrators. DDoS attacks continue on Ukrainian websites and on Ukrainian members of Parliament's cell phones. The Ukrainian Parliament agrees to a change in constitutional law and to return to the setting before the 2004 constitution.
22.02.2014	Ukrainian President Yanukovych flees to Russia. The Ukrainian Parliament elects Oleksandr Turchynov as acting President until the planned presidential election of 25th May 2014 (Pakharenko, 2015).
27-28.02.2014	Pro-Russian groups organize demonstrations in various Ukrainian cities, while non-uniformed soldiers seize airports and other strategic sites in Crimea. They cut off Crimean communications with the external world in a raid on the Ukrainian telecommunications infrastructures and tamper with its fiber optic cables (Gordon, 2014; Martin-Vegue, 2015).

[5] For a detailed table of the cyberattacks during this period and during the Ukrainian conflict, see Annex 1.

01.03.2014	The Russian Parliament authorizes the use of force against Ukraine (Lally et al., 2014).
02.03.2014	Russian troops enter Crimea (Maurer, 2015).
07-14.03.2014	Various Russian websites are targeted by DDoS attacks in retaliation for the invasion (Ukraine investigations, 2014).
16.03.2014	The referendum on the annexation of Crimea by Russia is carried by the Crimean population (Geers, 2015, p. 10).
16-18.03.2014	Various DDoS attacks on Ukrainian and Russian websites are reported (Ukraine investigations, 2014).
17.03.2014	The USA and European states agree on a first round of sanctions against Russia (Geers, 2015, p. 10).
18.03.2014	President Putin signs a bill on the annexation of Crimea (White, 2014).
04.2014	The war in the Eastern Ukrainian region of Donbass starts between pro-Russia separatists and the Ukrainian armed forces. At the same time, cyberattacks on Russian and Ukrainian websites continue. The USA and European states agree on a second round of sanctions against Russia (Shahani, 2015).
24.05.2014	A pro-Russian hacker named CyberBerkut hacks the servers of the Central Election Commission (CEC) and infects the election networks with malware. The Ukrainian cyber emergency response team manages to remove the malware from the network in time for the election (Weedon, 2015).
25.05.2014	Petro Poroshenko is elected as the new President of Ukraine (Geers, 2015, p. 10).
20.06.2014	President Poroshenko declares a seven-day ceasefire for the pro-Russian separatists to lay down their weapons. Cyberattacks from pro-Russian hacker groups also stop during this ceasefire (Shahani, 2015).
17.07.2014	Malaysia Airlines flight MH17 from Amsterdam to Kuala Lumpur is shot down by combatants in Ukraine resulting in approximatively 300 dead (Geers, 2015, p. 10).
07.2014	The USA and European states expand their sanctions against Russia (BBC News, 2014).
06.08.2014	Russia issues an embargo on agricultural goods from the countries that imposed sanctions against Russia (Walker and Rankin, 2014).
05.09.2014	The warring parties agree on a ceasefire in the Donbass region in the Minsk Protocol. The ceasefire collapses in January 2015.
25.10.2014	Poroshenko's political party wins the majority in the Ukrainian parliamentary elections. During the campaign, several DDoS attacks and hacks are observed against Ukrainian institutions (Martin-Vegue, 2015).
11.2014	Russia creates a new cyber warfare-specific military unit in Crimea (Pakharenko, 2015, p. 62).
12.2014	A new Russian military doctrine is published, which also details the concept of information warfare (Giles, 2016a, p. 27).
12.02.2015	The warring parties sign a new ceasefire agreement, the Minsk II Protocol. The protocol is violated shortly after it is signed (Weaver and Luhn, 2015).
03.2015	The EU creates a StratCom Task Force, whose goal is to identify and correct disinformation coming from Russian-speaking media (European Union, 2015).
23.12.2015	A cyberattack on the Ukrainian power grid leaves approximately 250,000 inhabitants without power for several hours (Zetter, 2016).
09.2016	An international investigation reports that flight MH17 was shot down by a Soviet-built BUK missile launched from the Donbass region (Harding, 2016).
25.10.2016	A Ukrainian hacker group leaks hacked emails from a key advisor of Vladimir Putin, Vladislav Surkov. His emails reveal that he was communicating with leaders of pro-Russian separatists in Ukraine on a regular basis (Windrew, 2016).
16.11.2016	Russia withdraws from the International Criminal Court (Reuters, 2016a).
01.12.2016	Ukraine tests missiles in the Black Sea, west of Crimea, and is accused of violating Russian territorial waters (BBC News, 2016a).
06-14.12.2016	Several cyberattacks target Ukrainian banks, state agencies and ministries (Miller, 2016a).

17.12.2016	Power goes out for an hour in the region of Kiev after a new cyberattack on the Ukrainian power grid (Goodin, 2017).
29.01.2017	In Eastern Ukraine, clashes between Ukrainian forces and separatist groups intensify after several calmer months (BBC News, 2017).

3 Description

This section describes the different tools and techniques used during the Euromaidan protests and the Ukrainian conflict to provide a better understanding of these tools and techniques, of how they work and the purposes they serve. It also explains who the targets of these cyberattacks were and who perpetrated them.

3.1 Tools and techniques

The cyberattacks in the conflict between Ukraine and Russia can be categorized by three types: DDoS attacks, website defacement and malware infection by spear phishing[6]. The first two tools are more accurately described as cyber-disruption, while the latter is oriented more strongly toward cyber-espionage for intelligence collection and battlefield preparation for further kinetic offensives or cyberattacks (Torruella, 2014, p. 121).

DDoS

An increase in DDoS attacks against various websites was observed at the beginning of the Euromaidan protests and during the invasion of Crimea. In a DDoS attack, perpetrators overload targeted websites with requests causing disruption to the website services and preventing legitimate users from accessing these pages. This technique requires the use of multiple computers infected by botnets or the coordination of a large number of users. Attackers control such computers compromised by botnets to send requests to the target network without users of infected computers even being aware of this. This kind of cyberattack was used multiple times by both parties to the conflict; Ukrainian media websites were targeted by pro-Russian hackers in November 2013, for instance, and Russian media websites were attacked by pro-Ukrainian hackers in December 2013. DDoS attacks can also serve as a distraction to monopolize the attention of the emergency team of the targeted institution. While they are busy combating the DDoS attack, the perpetrator(s) are able to conduct other malicious activities on the relevant network such as installing a backdoor or malware in order to steal data (NSFocus Inc., 2016, p. 4).

Website defacement

Website defacement has also been observed as a tool used by both parties in the Ukrainian crisis. This technique, where a hacker breaches a web server using an SQL injection to gain administrative access, is regarded as a cyber-version of vandalism. Once the system has been penetrated, the attacker changes the visual appearance of the website or replaces pages with their own materials. Hacktivists commonly use this technique to spread political messages. For instance, the website of the Russian media, RT, was defaced in March 2014, with attackers replacing the words "Russia", "Russian" and "military" with the word "Nazi" (Perlroth, 2014; Storm, 2014).

Malware

Various malware, believed to be linked to the Ukrainian conflict, has been observed throughout the conflict. The security firm FireEye reported that since the beginning of the war there has been an increase in the use of malware connected to Russian and Ukrainian servers (Geers, 2014). Four malware groups have been identified in this context: BlackEnergy, Snake[7], Operation Armageddon and X-Agent.

BlackEnergy

BlackEnergy is a family of malware primarily used by cybercriminals. It was also employed in a campaign named Sandworm (Zetter, 2014). The first version of BlackEnergy was used to gain access to networks in order to launch DDoS attacks. The second version, BlackEnergy2, was updated with new functionalities enabling it to steal data. The last version, BlackEnergy3, was updated to target Supervisory Control and Data Acquisition (SCADA) systems and added a new feature, KillDisk, which rendered the infected computers unusable. This version was used to attack the Ukrainian power grid system in December 2015 (E-ISAC, 2016; FireEye Inc., 2016). Attackers used spear phishing emails with a compromised attachment to infect computers. The malware would then install a backdoor to grant the attackers access to the network. The last two versions of the malware were deployed to gather information and were implanted in specific targets such as NATO, the Ukrainian government or the Ukrainian power grid system.

Snake

The Snake malware was discovered in 2014 but has been active since at least 2010 or 2011. It is similar to an older malware, Agent.btz, used to infiltrate the US military network in 2008. Victims got infected either by opening spear phishing emails or by visiting watering hole websites, i.e. webpages infected with malware in

[6] Even though the use of trolls to spread propaganda and misinformation is a technique used in the Russian information warfare, this aspect will not be considered as a tool for cyberattacks in this section. However, it will be examined in the section on attribution and actors.

[7] This malware is also known as Urobouros or Turla.

the hope that targets would visit it and get infected. Once the malware has infected a machine, it waits until the user opens a web browser and then simultaneously opens a backdoor for communication with the attackers without the user's knowledge (InfoSecurity, 2014; Paganini, 2014a). It is designed to copy and delete files, connect to infected servers, and to load and execute other malware. The Snake malware is composed of two elements: a rootkit and a driver. The former takes control of the computer and hides its activities from the user in order to steal data and capture network traffic. The driver injects code into the web browser to hide the exchange of information with the attackers' servers and creates a hidden file for holding configuration and stolen data (Paganini, 2014b; Symantec Security Response, 2014). The number of computers infected by Snake increased in Ukraine after the start of the Euromaidan protests. There were only eight cases of Snake infection in Ukraine in 2013, as compared to 14 new cases between January 2014 and March 2014. A total of 32 cases have been observed since 2010 (Sanger and Erlanger, 2014).

Operation Armageddon

Operation Armageddon is a Remote Administration or Access Tool (RAT) that targeted Ukrainian government, law enforcement and military networks. It was discovered in September 2014 by the US security firm LookingGlass. Security experts and Ukrainian officials suspect Russia of creating and using this malware (Witty, 2015). Its purpose was to gather information about its victims, probably to gain the advantage on the battlefield in Eastern Ukraine (Weedon, 2015, p. 72). This practice demonstrates that cyberespionage can be used as a tool to support physical warfare. It is believed that this malware has been active since at least 2013, when Ukraine started discussing an Association Agreement with the EU. It infected machines through spear phishing emails with a compromised Microsoft Word attachment. It has been noted that some stolen documents were injected with the malware and sent to new targets of spear phishing emails (Hackett, 2015).

X-Agent

X-Agent is a malicious application found on Android and Apple smartphones. It was revealed to the public in December 2016 but has been active since 2013. The application was first created as a legitimate software by a Ukrainian artillery officer in order to prepare artillery targeting data faster. The legitimate application was used as a decoy for malware that intercepts communications and gives away users' locations without their knowledge. According to the cybersecurity firm Crowdstrike, this malicious application was developed by the hacker group APT28 (Crowdstrike, 2016).

3.2 Targets

In this series of cyberattacks, there were various victims, but most were located in Ukraine and Russia. In this analysis, victims are categorized by activity and country of origin: Ukrainian institutions, Ukrainian media outlets, Russian institutions, Russian media outlets, Russian groups, and third parties.

Ukrainian institutions sustained various kinds of cyberattacks during the Euromaidan protests and during the war with Russia. During the invasion of Crimea, the government website was down for 72 hours because of a DDoS attack, and the cell phones of the members of Parliament were overwhelmed with SMS to prevent them from communicating to coordinate a response. The attacks were not limited to DDoS and defacement of websites. Government networks were also targeted by malware campaigns such as Snake and Sandworm. Ukrainian institutions were targeted by malware for intelligence gathering, protest or retaliation with DDoS (Ukraine investigations, 2014; Weedon, 2015).

Ukrainian media outlets, newspapers, TV channels, and news agencies suffered mostly from DDoS attacks and website defacement during the Euromaidan protests and during the early stages of the war. They were targeted to either prevent them from reporting events or as retaliation for the way they portrayed events (Ukraine investigations, 2014; Weedon, 2015).

Russian institutions sustained mostly DDoS attacks and website defacement from Ukrainian hacker groups. For example, at the beginning of the war, both the Kremlin website and the website of the lower parliamentary chamber fell victim to a DDoS attack. They were mainly targeted in retaliation for Russia's actions in Ukraine and Crimea. More recently, they suffered data theft by a Ukrainian hacker group, Cyber Hunta. This group stole emails from one of President Putin's advisors, revealing links between the Kremlin and separatists groups in Eastern Ukraine (Windrew, 2016).

Russian media outlets suffered mostly from DDoS and defacement attacks. The goal would have been to either disrupt websites through DDoS attacks, or to expose the media websites to ridicule by defacing them.

Third parties include NATO, the Organization for Security and Co-operation in Europe (OSCE), and organizations and countries not directly involved in the conflict that were still victims of various cyberattacks related to the Ukrainian conflict. Various NATO websites were hit by DDoS attacks at the start of the war, and NATO servers were infected by the same malware that infected Ukrainian institutions, i.e. Snake and Sandworm. The former has also been found in Belgian, Lithuanian and British networks (Paganini, 2014a). NATO was probably also targeted for intelligence collection. The DDoS attacks could additionally have been made in retaliation or as a signal for NATO to stop its enlargement (Giles, 2015). The OSCE, which discovered spying malware in its system in November 2016, was probably targeted to gather information on observers operating in Ukraine or elsewhere in the world (BBC News, 2016b). The Dutch Safety Board was targeted for several days as it released its report on the investigation of the crash of flight MH17 (Foxall, 2016). It might have been targeted to protest and disrupt the publication of the report.

3.3 Attribution and actors

Attribution in cyberspace remains a complicated task. It normally follows the *cui bono* (to whose benefit) logic, but there will always be uncertainty regarding perpetrators. The sources used for this report are mainly academic journals, major Western media and cybersecurity firms. However, there is the possibility that technical evidence found may have been set up in a certain way by certain actors in order to incriminate others.

In the specific case of the Ukrainian conflict, the attribution issue is especially complicated because of the volume of attacks and the fact that both sides use proxies. The use of proxies gives states the advantage of plausible deniability: If attacks are successful, the state benefits from the results of the attacks. However, if they fail, or are compromised, the state can dissociate itself from these groups by declaring that they acted on their own initiative without any government support (Maurer, 2015, p. 81). The distinction between state actors and non-state actors is also unclear, as both tend to share tools. For instance, it was reported that the BlackEnergy toolkit was normally used by cybercriminals for DDoS attacks. However, the attack on the Ukrainian power plant showed that this tool can also be used for espionage and to gain access to political targets (F-Secure, 2014).

Actors come from both states and can be categorized into two groups: pro-Ukrainian hacker groups and pro-Russian hacker groups. The difference between the two categories is not geographical because some groups target their own country's institutions. Moreover, some pro-Russian hacker groups perpetrated their attacks from the Eastern Ukrainian territories to bypass territorial filters blocking Internet Protocol (IP) addresses coming from Russia (Ukraine investigations, 2014).

The following list is non-exhaustive and only details the main active groups on both sides. There is the possibility that some of these groups are in fact the same but operate under different names and have therefore been categorized as two different groups.

Pro-Ukrainian hacker groups

- Cyber Hunta: A hacktivist group composed of several volunteers whose goal is to expose Moscow's involvement in the conflict in Ukraine. They claim not to be associated with the Ukrainian government (Miller, 2016b).
- Cyber Hundred[8]: This hacktivist group aims to remove pro-Russian trolls from Ukrainian websites and to protect Ukrainian websites from pro-Russian hackers. They teach the population about ways to fight trolls and help to retaliate against cyberattacks (Ukraine investigations, 2014). However, very little is known about their structure or their members.
- Null Sector: This hacker group was created after the fall of the former Ukrainian President Yanukovych in February 2014. They mostly use DDoS attacks against Russian websites and offer their services to fight back against cyberattacks (Ukraine investigations, 2014).
- Ukrainian Cyber Troops/Army: This hacker group, which was founded by Eugene Dukokin, a former cybersecurity consultant and programmer (Maheshwari, 2015), targets pro-Russian separatists and Russian troops in Ukraine. They report accounts of pro-Russian officials to various banking and payment websites or social media in order to get the accounts closed. These actions are legal and do not require them to hack any systems (Kerkkänen and Kuronen, 2016).

Pro-Russian hacker groups

- CyberBerkut: This hacker group supports separatist groups in Eastern Ukraine, but it remains uncertain whether it is composed of pro-Russian Ukrainians or Russians. CyberBerkut has claimed to be behind several cyberattacks, ranging from DDoS of NATO websites to the implantation of malware into the CEC. Rumors have it that former members of the Ukrainian special police forces, Berkut, are behind CyberBerkut. Others claim that CyberBerkut is in reality the Russian hacker group APT28 (Miller, 2016b) or that they work together against common enemies (Ashok, 2016). It is said that CyberBerkut benefits from expertise and funding from the Russian government (Kerkkänen and Kuronen, 2016).
- APT28[9]: This hacker group was first discovered in 2008 during the conflict between Russia and Georgia. The group is believed to have ties to the

[8] This hacker group is also known as KiberSotnya or CyberMaidan.

[9] This hacker group is also known under the names Sofacy, Fancy Bear, Pawn Storm, Strontium or Sednit.

Russian Main Intelligence Directorate (GRU), which is the foreign military intelligence office. They are highly professional and use malware developed on computers with Russian language settings. They are known to design their malware to fit their targets and to use spear phishing to infect their victims, as well as using zero-day vulnerabilities. They have infiltrated the networks of Russian dissidents, European security organizations, defense contractors, Western governmental institutions, and media outlets. They are one of the two groups who allegedly hacked into the US Democratic National Committee in 2016[10]. The choice of their targets seems to be the typical targets that a military intelligence service like the GRU would concentrate on. APT28's malware has been found in Ukrainian government networks and artillery troops' smartphones (Crowdstrike, 2016; Koval, 2015; Weedon, 2015). The security firm ThreatConnect believes that they are linked to CyberBerkut, as the two groups took turns in spear phishing campaigns against the investigative journalist group Bellingcat (Ashok, 2016).

- APT29[11]: This hacker group was first seen in 2008 during a series of cyberattacks in Chechnya. They have also been accused of breaches of the US State Department and the US White House (Thielman and Ackerman, 2016). They are believed to have ties to the Russian Federal Security Services (FSB), the main Russian national security institution and successor to the KGB. They are known to use spear phishing techniques and often reuse stolen documents from previous hacks to lure and infect new victims. APT29 is believed to use a backdoor malware called Hammertoss to stealthily retrieve information; however, there is no information regarding the use of Hammertoss in the Ukrainian conflict (Standish, 2015; Weedon, 2015). They are considered to be highly professional and meticulous in their actions, constantly trying to reduce or eliminate any forensic evidence. This level of organization and the use of highly sophisticated software suggests that they are state-financed (FireEye Inc., 2015).
- Anonymous Ukraine: This hacker group is the branch of the hacktivist movement Anonymous in Ukraine. It is, however, internally divided in its position regarding the conflict in Eastern Ukraine. Some of its members are pro-Ukrainian and tend to be close to Cyber Hundred and Null Sector, while others are pro-Russian and close to CyberBerkut. The pro-Russian element is prominent, having claimed several attacks on NATO, US and EU governments' websites (Carr, 2014).
- Quedagh: This name has been assigned to this group by analysts from the security firm F-Secure, after the group employed the BlackEnergy toolkit against political targets. F-Secure suspects that the group was also involved in the conflict between Russia and Georgia in 2008. The hacker group has used different versions of the toolkit since 2010. The evolution of their version of the toolkit shows that they take a patient approach and closely observe their victims to fine-tune their malware to their targets (F-Secure, 2014, p. 4).
- Trolls: Trolls are used by the Russian government to spread pro-Russian propaganda in social media, blogs and forums abroad and in Russia. They are organized in "troll farms or factories", i.e. institutions from which trolls post their messages, comments or posts. One of these troll farms was discovered in St. Petersburg, where trolls were arranged in sectors responsible for different media and given quotas for comments and posts to be written per day. The Ukrainian government and Ukrainian conflict are said to constitute the most prominent topics targeted by trolls (Volchek and Sindelar, 2015).
- Nashi Youth Movement and Russian Patriotic Hackers: "Nashi" means "ours", and the Nashi Youth Movement was a political youth movement for young Russians aged between 17 and 25 years. The organization was created in 2005 in response to the activist movement of the Orange Revolution in Ukraine. The movement was openly pro-Putin and was reported to have harassed and spied on opposition activists (Shachtman, 2009). The movement was terminated after the resignation of its president following changes in the Russian government in 2012 (Hartog, 2016). The group claimed responsibility for the cyberattacks on Estonian institutions in 2007 and was also known to have organized pro-Russian protests in Finland and Estonia (Stratfor, 2012). Even though the movement was terminated in 2012, some of its members may continue to be involved in cyber-activities as patriotic hackers, individuals or groups of individuals perpetrating hacking activities on their own initiative against what they perceive to be enemies of Moscow (Denning, 2011, p. 178).

[10] For more information about the Democratic National Committee hack, please see: Baezner, Marie; Robin, Patrice (2016): Hotspot Analysis: Cyber-conflict between the United States of America and Russia, December 2016, Center for Security Studies (CSS), ETH Zürich.

[11] This hacker group is also called Cozy Bear, The Dukes or CozyDuke.

4 Effects

This section analyzes the various effects of the cyber-aspect of the Ukrainian conflict on the Ukrainian domestic and international levels. At the Ukrainian domestic level, the report looks at the damage to society caused by cyber-activities in the context of the conflict. It also focuses on the economic costs of such cyberattacks for the private sector and governmental institutions. It further examines both the technological damage resulting from the conflict and technological innovations resulting from it.

At the international level, this section focuses on the international effects of the cyberattacks and the Ukrainian conflict on the international order and cooperation.

4.1 Social and political effects

On the social level, people from East Ukraine and Crimea, which are mostly Russian-speaking regions, are totally isolated from any outside information. They are only able to listen to Russian radio or watch Russian television and therefore have very limited access to other forms of media, effectively preventing them from forging other opinions than those promoted by Russian media. On the other hand, people from the Western part of Ukraine have limited access to Russian-speaking media (Lange-Ionatamishvili and Svetoka, 2015; Nocetti, 2015; Selhorst, 2016). Maintaining this isolation is an important part of Russian information warfare, where the goal is to control public opinion and indirectly shape decisions in favor of Russia (Lewis, 2015). Russian propaganda is judged to be highly effective. It broadcasts through a large number of channels, ranging from traditional television to social media and chat rooms. This enables propaganda to reach a larger number of people and publish news faster than traditional media channels limited by the need to check facts before publication (Paul and Matthews, 2016). Propagandists also try to increase the credibility and visibility of their news platforms by inviting experts or celebrity guests, such as Julian Assange and Larry King (Besemeres, 2014).

The significant volume of cyberattacks on Ukrainian institutions most likely also strained people's faith in these institutions and intensified a general feeling of insecurity. DDoS attacks and defacement erode people's trust in their institutions and their ability to protect their own population. This is also the logic behind the creation of various hacker groups in Ukraine, including Dokukin's Ukrainian Cyber Troops/Army. At the beginning of the conflict, the Ukrainian authorities visibly lacked the capacity to deal with the various cyberattacks. As a consequence, private initiatives such as Dokukin's decided to support the government and the Ukrainian people against trolls and other Russian cyber activities (Kerkkänen and Kuronen, 2016). Another good example of diminishing people's trust in their government was the distributed denial of telephone service attack launched on the call center of the Ukrainian power supplier during the blackout of December 2015. The call center was flooded with fake phone calls, rendering it unable to answer legitimate calls from customers experiencing power outages. This situation led Ukrainians to believe that Ukrainian energy suppliers are not prepared for incidents of this nature (Zetter, 2016).

4.2 Economic effects

The economic effects of the cyberattacks in the context of the Ukrainian conflict mostly concern the consequences of the DDoS and defacement attacks. DDoS attacks usually generate direct costs for businesses in the form of loss of revenue and loss of productivity. The average economic damage is estimated to be US$22,000 per minute of website unavailability, and the average estimated duration of these attacks was 54 minutes (Kenig, 2013). Such attacks can therefore cost a substantial amount of money for the businesses they target. However, every business is affected differently by DDoS attacks, and other costs such as investigation, technical response, customer support and public relations costs further add to the bill. Indirect costs, including damage to reputation, theft of critical data and opportunity costs, also need to be taken into account and can also have serious consequences (NSFocus Inc., 2016). In the context of the Ukrainian conflict, the victims of such attacks were mostly media outlets, banks and governmental websites. For the first two types of victim, loss of revenue may be the most important concern, while for government institutions whose websites were targeted, reputational damage and the indirect costs incurred by such attacks constitute the most urgent issues. In their cases, people may begin to doubt the institutions' ability to perform their tasks or protect the public (especially where institutions were unable to protect their own websites from a cyberattack).

Website defacement has similar economic consequences to DDoS attacks. If defacement involves a redirection of visitors to another website, the targeted webpages may lose customers while the defacement persists. Defacement additionally causes a loss of trust in the owners of defaced websites. This type of attack exposes weaknesses in webpage security, which may suggest further vulnerabilities and thus render sites and site owners untrustworthy (Paladion Networks, 2015).

Malware infections can be just as economically damaging as DDoS attacks for victims. However, it seems that in the Ukrainian conflict malware was used for collecting information for intelligence purposes and not for enrichment or cybercriminal activities. These intrusions cause similar costs to DDoS attacks because victims need to engage emergency teams to stop the interference and investigate the attack. They also impact on institutions' reputations for the same reasons as DDoS and defacement attacks (BanffCyber Technologies, 2016).

4.3 Technological effects

In the context of the conflict in Ukraine, there were physical attacks on telecommunications infrastructures as well as cyberattacks on critical infrastructures. In particular, when Ukraine was invaded in March 2014, the so-called "little green-men" raided the Crimean infrastructures of the Ukrainian telecommunications provider, UkrTelecom. They tampered with the Crimean internet exchange point in order to isolate the peninsula from the rest of the world and prevent it from communicating events. In this instance, the physical damage caused was not the result of a cyberattack, but rather of a material interference with the functioning of the internet in Crimea. Russia, which admitted that the "little-green-men" were in fact Russian troops in April 2014, did not try to shut down the internet in Ukraine entirely for two reasons (Karmanau and Isachenkov, 2014). First, it would have been too difficult because Ukraine has six internet access points, all of which go through Kiev. Second, Russia already owns the main telecommunications companies in Ukraine, which also rely mostly on Russian hardware for their telecommunications infrastructures (Libicki, 2015, p. 50; Tucker, 2014). Furthermore, many Ukrainians use Russian social media such as vKontakte and Russian internet resources such as email addresses, allowing the Russian authorities to intercept and read or listen to all conversations conducted via these platforms. Even some Ukrainian officials used email accounts provided by Russian companies, which allowed the Russian government to easily obtain the information it needed even without cyberattacks (Pakharenko, 2015; Poludenko-Young, 2015). This partly explains why there have been so few attacks on communications infrastructures in the physical and cyber realms and illustrates that technological dependence on another state can have significant consequences.

The first cyberattacks on critical infrastructures occurred in December 2015, when several Ukrainian power plants were shut down for several hours. The attacks involved the BlackEnergy3 malware. Investigators reported that the power plants targeted were still not back to full production levels even two months after the attacks. The attackers overwrote the firmware code for 16 substations, resulting in operators being unable to log into the substation systems remotely and needing to control them manually. Furthermore, the malware contained a payload named KillDisk, which erased and crashed infected computers. Infected machines could not be restarted. All stored data and information was lost and needed to be replaced.

This particular attack on power plants may have been a response to the physical attack of a pro-Ukrainian group on power substations in Crimea. However, the forensic investigation showed that the infection already started in spring 2015. Investigators claimed that the attackers could have done significantly more damage than merely shutting down power for several hours. They assume that the attack was only a message to show off their capabilities (Zetter, 2016).

The second cyberattack on critical infrastructures occurred in December 2016 and was very similar to the one from the year before. It targeted a power plant near Kiev and caused a power outage for approximately one hour. The attack used both the same BlackEnergy malware and KillDisk payload. The malicious software was planted in the system via a spear phishing campaign. However, the incident caused less significant material damage than the one in 2015 (Goodin, 2017).

The techniques used in cyberspace in the Ukrainian conflict are not new and did not reach the same intensity as during the conflict between Georgia and Russia in 2008 (Perlroth, 2014; Weedon, 2015). The novel element in this conflict was the emergence of new malware, including Snake, Operation Armageddon and X-Agent, which also revealed the development of criminal malware such as BlackEnergy for intelligence and offensive operations. The discovery of malware targeting smartphones, i.e. X-Agent, was another significant technological development during the conflict. This represents a completely new element in the dimension of intelligence collection and communication on the battlefield. These new types of malware could trigger a cyber-arms race among states fearing cyberattacks from Russia. These states might build new cyber-defensive measures or offensive capabilities in order to defend themselves. There is also the risk that the malware used during the conflict may be deployed for criminal purposes.

4.4 International effects

After the Euromaidan protests and subsequent annexation of Crimea in March 2014, the number of cyberattacks relating to Ukraine and Russia increased. Given this intensity, people were expecting to see the development of a cyberwar between the two states, but this scenario never eventuated. In reality, the conflict occurred simultaneously in cyberspace and the physical world: cyber-means were used in combination with, and in support of kinetic operations. In this instance, a possible pattern of escalation of activities in cyberspace and a spilling over into the physical realm did not occur because the conflict escalated in parallel in both spheres. Cyber-operations were used in advance in order to support kinetic operations through the collection of intelligence and misinformation. Moreover, the cyberspace aspect of the conflict was significant at the beginning of the war, then settled down and has remained at a more or less constant level of intensity since. The cyberattacks were mainly limited to cyber-disruptive and enabling operations attacks such as DDoS, website defacement, and intelligence collection malware (Torruella, 2014, p. 121). Intensity seems to have picked up again since December 2015, but even in these cases damage was intentionally limited. The cyberattacks on the Ukrainian power grid in December 2015 and 2016 could have caused an escalation in the conflict; however, the attackers limited the damage they caused. A US Air Force expert who assisted the Ukrainian authorities with their investigations stated that the attackers could have done a lot more damage but stopped their attack after a few hours (Zetter, 2016). The expert suggested that both attacks were merely intended to show what the perpetrators were capable of. This self-limitation can also be understood as a way of avoiding further escalation of the conflict, which would risk a significant response from Ukraine or its allies. Critical infrastructures and human lives are considered as “red lines” not to be crossed if actors wish to contain a conflict (Lin, 2012).

The conflict in Ukraine has shown that Russia is ready to use military force as a foreign policy instrument, as it did in 2008 during the conflict between Georgia and Russia. At the same time, the use of cyber-means by Russia has developed since the 2008 conflict in the Caucasus. Following the conflict with Georgia, Russia created an “information platoon”, which was later transformed into troll farms (Giles, 2016a, pp. 29–30). However, the conflict in Georgia was different in that Russia had more trouble controlling the “information space” in 2008 and was perceived as having lost the information war (Nocetti, 2015, p. 26). On the other hand, Ukraine found itself completely isolated from outside information in 2014, and it was difficult for foreign media to obtain accurate information about what was happening in the country. The fact that Western media were unable to confirm the presence of Russian military in Ukraine essentially throughout 2014 proved that the Russian tactic of isolating Ukraine’s “information space” had become more effective compared to 2008. While Western countries judged Russian propaganda and misinformation to be too obvious and easily identifiable, Russians were able to pollute information feeds, causing confusion about the reliability of information coming from the region (Giles, 2015, pp. 25–27). Russia also made use of its proxy forces in the physical part of the conflict in Ukraine to complicate the situation. This gave Russia the ability to deny any physical involvement in the conflict. This method was also successfully deployed in cyberspace, as evidenced by the presence of CyberBerkut, which some sources claimed to be a pro-Russian hacker group from Ukraine, while others asserted that it was in fact a Russian hacker group, APT28 (Koval, 2015, p. 57).

At the international level, Ukraine found itself isolated from any help and at the mercy of efficient Russian information warfare following the annexation of the Crimean. In December 1994, the USA, Great Britain, France and China promised Ukraine, in the Memorandum on Security Assurances, that they would seek assistance from the UN Security Council if there was any aggression from Russia (United Nations, 1994). In reality, the former Soviet Republic is geographically too close to Russia and too far from Western Europe to benefit from any significant military support from Western states. Apart from some material and educational help, Western countries’ armies have not done much to prevent Russia from annexing Crimea or to stop the conflict in Eastern Ukraine (Besemeres, 2014). Assistance from NATO came in the form of funding and expertise to protect Ukraine’s cyberspace, but no NATO troops were deployed. In September 2014, the NATO Summit agreed to create five funds to assist Ukraine, one of which is the Cyber Defense Trust Fund aimed at training personnel and advising Ukrainian authorities on cyber-policies (Fiscutean, 2015). NATO also conducts regular international military exercises in the Ukrainian region in order to demonstrate that the region has not been forgotten. The USA also assists Ukrainian forces by training troops and donating equipment such as radars, Humvees and medical supplies (Gould, 2015).

Western states did, however, impose economic sanctions on Russia after the annexation of Crimea. These sanctions were not forced on Russia specifically because of the cyberattacks in Ukraine. Nevertheless, the bans and embargos had some impact on the Russian economy. The goal of these sanctions was for Western states to put pressure on Russian markets over the long term to show their condemnation of the war in Ukraine and the annexation of Crimea. The sanctions restricted access to European and American capital markets by Russian financial, energy and defense businesses, an import and export ban on arms trading, an export ban on dual-use goods, restricted access to sensitive technologies, and a restriction on services linked to oil production (Gros and Mustilli, 2016). These sanctions had an impact on the Russian economy, causing it to contract by 1.5% in 2015, but their effect has in fact been limited. In reality, the fall in oil prices in 2015 had a stronger impact on the Russian economy than the sanctions (Emmott, 2016). Yet the sanctions have put presssure on the Russian economy, albeit without influencing Russian policy regarding Ukraine.

5 Policy Consequences

This section proposes several measures that states can apply to decrease the potential impact of activities similar to the Ukrainian conflict occurring in cyberspace.

5.1 Raising awareness of propaganda and misinformation

Throughout the conflict, Russia has used a combination of cyber, EW, intelligence and kinetic capabilities to control communications within or from Ukraine (Giles, 2016b). This comprehensive approach needs to be acknowledged and understood in order to better counter it.

Based on this case, a primary danger was Russia's focus on information warfare using propaganda, systematic internet trolling and misinformation. It is important that states admit that such cyber-activities may be less sophisticated technically than direct cyberattacks on critical infrastructures but can also do a great deal of damage in society. This issue needs to be debated openly among the highest political circles in order to raise awareness among political leaders and society, as it is difficult for democracies to counter propaganda. Freedom of the press and free speech are core democratic principles, but they also provide a space in which propaganda and misinformation can easily spread. Russian media outlets such as RT or Sputniknews understand this vulnerability and readily exploit it.

In addition to an open debate on misinformation and propaganda, states can take other measures to mitigate the effects of these tactics. However, it is essential for democracies to truly understand the effects of propaganda and misinformation if they are to counter these tactics effectively and be able to develop effective awareness programs. Such programs should explain to the population the difficulties surrounding information warfare. While government agencies may wish to warn domestic audiences about disinformation campaigns and provide tips on how to detect and denounce them, they must also integrate other actors, including the media. They should also clarify what trolls are and what role they play in propaganda operations (Tatham, 2015). Education and awareness campaigns can be designed to help the population to discern propaganda materials more readily and take a more critical stance toward what they read or watch. It would also be important for democracies to reveal and correct misinformation and inconsistencies in news in order to limit the effects of propaganda (Paul and Matthews, 2016).

5.2 Limit dependence on foreign technology

The case of the Ukrainian conflict has shown that reliance on foreign technology in operating critical infrastructures could be fatal in case of conflicts. It is therefore important to restrict dependence on foreign companies for hardware or software to a minimum as far as possible. Relying on foreign technology is problematic for both security and logistic reasons. For example, a foreign supplier may need to travel to the country for maintenance or to update a product. This might provide them with an opportunity to collect intelligence on how the product is used and its purposes. They might also be tempted to sell information they collect to other states. In terms of state security, it is preferable to produce hardware and software domestically if a state has the relevant ability and capacity. Where this is not possible, states should prioritize the security aspects of such actions. Independent hardware and software checks should be performed regularly or inserted into foreign assets to detect any real and perceived vulnerabilities left (intentionally or accidentally) by the supplier.

The fact that a significant proportion of Ukrainians use email services provided by Russian companies also facilitated the collection of intelligence by Moscow. The fact that foreign email service providers are easily able to read and store email discussions and information needs to be highlighted and explained to users. Education and awareness campaigns may be helpful in raising awareness of this issue among the population. Governments could also suggest domestic alternatives or encourage companies to develop them.

The physical attack on the Ukrainian communications infrastructure in Crimea underlined the fact that the protection of such infrastructures needs to be addressed in combination with cyber strategies, especially since there have been reports that Russia showed interest in submarine internet cables, land telecommunication links and communications satellites. This type of attention could be aimed at collecting intelligence on infrastructure vulnerabilities or at obtaining access to the information carried via such infrastructures (Giles, 2016b, pp. 11–13).

5.3 Leading by example against DDoS and website defacement

DDoS attacks and website defacement were frequently used during the Ukrainian conflict. While these forms of attacks are only regarded as cyber-disruptions, they can still be expensive for victims. Governments should lead by example in terms of website security, thereby boosting their credibility and encouraging private actors to implement proper website security. It is also important that states with relevant capabilities assist other actors that might be less capable of dealing successfully with attacks. A standard operating procedure could be created to guide businesses in case of DDoS or website defacement.

5.4 Monitoring of the evolution of the conflict

Western states are not direct victims of cyberattacks from either party of the conflict, but private companies and individuals may be indirectly affected. States that are active on the mediation scene in Ukraine through the OSCE might be specifically targeted. Their involvement increases the risk of falling victim to future cyberattacks. As a matter of a fact, the OSCE was targeted by a cyberattack allegedly perpetrated by Fancy Bear in December 2016 (BBC News, 2016b; “What Effect Will U.S. Sanctions Have On Russia?,” 2016). States should closely monitor the cyber-activities in the Ukrainian region to evaluate if the risk of direct and indirect cyberattacks on their infrastructures, individuals or businesses increases.

5.5 Confidence Building Measures (CBMs)

The promotion of CBMs in cyberspace in times of peace and war could help to reduce uncertainties and misperceptions. So far, states have merely agreed that international law could apply to states’ activities in cyberspace, but CBMs could help to increase trust and transparency among states in cyberspace. The difficulty of attributing actions to actors in cyberspace can raise ambiguities that may lead to further international tension. Clearer international protocols, agreements or guidelines negotiated through bi-lateral processes or in regional/international forums may help to mitigate relevant issues. Stauffacher and Kavanagh (2013) proposed a series of CBMs in the context of cybersecurity consisting of:

- Transparency measures (dialog on cyber policies/strategies/doctrine, exchange of military personnel, joint simulation exercises, and so forth); compliance indicators and monitoring of transparency measures (e.g. agreement on prohibited targets such as hospitals, joint mechanisms in crisis management such as hotlines).
- Cooperative measures (e.g. development of common terminology, development of joint guidelines in case of incidents, joint threat assessments).
- Communication and collaborative mechanisms (e.g. communication channels in case of escalation).
- Restraint measures (e.g. pledge to remove incentives for first strike offensive or retaliation actions, exclusion of cyber offensive operations on third parties countries).

Such measures would also enhance cooperation among states and result in greater dialog, which could also evolve into international norms or treaties. This in turn could improve security in both the cyber and the physical realms (Brake, 2015; Farrell, 2015; Stauffacher and Kavanagh, 2013).

6 Annex 1

Non-exhaustive table of the various cyberattacks occurring during the Ukrainian Euromaidan protests and the conflict with Russia:

G = Government institutions, M = Media outlets, IO = Intergovernmental Organization, O = Others				
Date	**Victim**	**Type of victim**	**Alleged perpetrator**	**Technique/Tool**
07.11.2013	CCDOE website	IO	CyberBerkut or Anonymous Ukraine	DDoS (Carr, 2014)
15.11.2013	Ukraine Customs Services	G	Anonymous	Unspecified data breach (Kovacs, 2013a)
24-25.11.2013	Newspaper Ukraiska Pravda website	M	Pro-Russian actor	DDoS (Ukraine investigations, 2014)
26.11.2013	TV channel Hromadske website	M	Pro-Russian actor	DDoS (Ukraine investigations, 2014)
26.11.2013	News website censor.net	M	Pro-Russian actor	Wiped all information on the website (Ukraine investigations, 2014)
31.11.2013	Ukrainian Ministry of Internal Affairs website	G	Protesters of the Euromaidan movement	DDoS (Ukraine investigations, 2014)
04.12.2013	Pro-Russian news website of Ukrainskaya Pravda	M	Pro-Ukrainian actor	DDoS (Ukraine investigations, 2014)
10.12.2013	Ukraine Brovary region website	G	Anonymous affiliated group called Clash Hackerz	Unspecified data breach and defacement (Kovacs, 2013b)
28.12.2013	Emails from the Ukrainian Volyn regional state administration website	G	Anonymous	Credentials and passwords for email accounts obtained by a phishing campaign (Johnstone, 2013)
07.01.2014	Ukrainian TV 5 Channel News website	M	Pro-Russian actor	DDoS (Ukraine investigations, 2014)
09.01.2014	The webpage maidan.ua.org	O	Pro-Russian actor	DDoS (Ukraine investigations, 2014)
16.01.2014	Website of the Greek-Catholic Church in Ukraine	O	Pro-Russian actor	DDoS (Ukraine investigations, 2014)
28.01.2016	Ukrainian TV channel website espresso.tv	M	Pro-Russian actor	DDoS (Ukraine investigations, 2014)
31.01.2014	30 Ukrainian government and media websites	G/M	Ukrainian neo-fascist party Svoboda	Defacement (Waqas, 2014)
11.02.2014	A regional office of the Ukrainian Democratic Alliance for Reform party	O	Anonymous	Unspecified data breach (Johnstone, 2014)

Date	Victim	Type of victim	Alleged perpetrator	Technique/Tool
18.02.2014	Ukrainian members of Parliament's cell phones	G	Unknown	Cell phones flooded by SMS to prevent members of Parliament from using their phones (Weedon, 2015)
27-28.02.2014	Ukrtelecom infrastructures in Crimea raided	O/G	Armed "little-green-men" (presumed Russian special forces troops)	Cutting cables (Martin-Vegue, 2015)
03.2014	Ukrainian government's website	G	Unknown	Shut down for 72 hours (Weedon, 2015)
03.2014	Ukrainian media outlets' websites	M	Unknown	DDoS (Weedon, 2015)
03.2014	Ukrainian government's network	G	Unknown	Snake malware (Sanger and Erlanger, 2014)
02.03.2014	Pro-Russian news website RT.com	M	Unknown	Defacement, replacing certain words by "Nazi" (Perlroth, 2014)
04.03.2014	Ruptly (a video website part of RT)	M	Unknown	DDoS (Kovacs, 2014)
07.03.2014	The Kremlin's website	G	Cyber Hundred or Null Sector or another pro-Ukrainian actor	DDoS (Maurer, 2015)
14.03.2014	Russian President's website and Bank of Russia's websites	G	Cyber Hundred or Null Sector or another pro-Ukrainian actor	DDoS (Ukraine investigations, 2014)
14.03.2014	Russian news portal lenta.ru	M	Cyber Hundred or Null Sector or another pro-Ukrainian actor	DDoS (Ukraine investigations, 2014)
16.03.2014	Several NATO websites	IO	CyberBerkut	DDoS (Bejtlich, 2015)
18.03.2014	Regional TV of Rivne in Western Ukraine	M	CyberBerkut	DDoS (Ukraine investigations, 2014)
18.03.2014	Ukrainian news portal zik.ua	M	Pro-Russian actor	DDoS (Ukraine investigations, 2014)
24.03.2014	7 million credit cards	O	Anonymous	Data breach and leak (Passeri, 2014a)
03.04.2014	Website of the Coordination Council of Sevastopol	G	Pro-Ukrainian actor	Defacement and rerouting (Ukraine investigations, 2014)
04.04.2014	Websites of Ukrainian Main Prosecutor Office and of Ukrainian Ministry of internal Affairs	G	CyberBerkut	DDoS (Ukraine investigations, 2014)
09.04.2014	Ukrainian Main Prosecutor's Office's webpage	G	CyberBerkut or another pro-Russian actor	DDoS (Ukraine investigations, 2014)
09.04.2014	Ukrainian blog RoadNews	M	Pro-Russian actor	DDoS (Ukraine investigations, 2014)
10.04.2014	The Russian Lower Parliament Chamber's (Duma) website	G	Pro-Ukrainian actor	DDoS (Ukraine investigations, 2014)
05.2014	Ukrainian Privatbank	O	CyberBerkut	Data theft (The Moscow Times, 2014)

Date	Victim	Type of victim	Alleged perpetrator	Technique/Tool
25.05.2014	Ukrainian Central Election Commission's website	G	CyberBerkut	Defacement and unspecified malware (Koval, 2015; Weedon, 2015)
26.07.2014	Email of the Ukrainian Colonel Pushenko	G	CyberBerkut	Data breach and leak (Passeri, 2014b)
09.08.2014	Regional department of the law enforcement in Dnepropetrovsk, Ukraine	G	CyberBerkut	Data breach and leak (Passeri, 2014c)
10.2014	Ukrainian Central Election Commission's website	G	Unknown	DDoS (Martin-Vegue, 2015)
24.10.2014	City billboard in Kiev	G/O	CyberBerkut	Depiction of Ukrainian members of Parliament as war criminals (Lange-Ionatamishvili and Svetoka, 2015)
20-21.11.2014	Several Ukrainian governmental websites	G	CyberBerkut	Defacement of the websites with a message on Joe Biden being a fascist (Shevchenko, 2014)
2015	Bellingcat	O	APT28	Spear phishing campaign (Ashok, 2016)
02.01.2015	Ukrainian law enforcement and justice organizations	G	Anonymous	Data breach and leak (Passeri, 2015a)
27.02.2015	US private military contractor involved in Ukraine, Green Group Defense Service	O	CyberBerkut	Access to information on phones (Passeri, 2015b)
25.04.2015	Ukrainian government network	G	Unknown	Operation Armageddon malware (Bejtlich, 2015)
04-05.2015	Ukrainian Ministry of Defense	G	Unknown	Targeted intrusions into the network (Crowdstrike, 2016, p. 5)
13.10.2015	The Dutch Safety Board (investigative body for the crash of flight MH17)	O	Allegedly APT28	Spear phishing and another unspecified type of cyberattack (Foxall, 2016)
18.08.2015	Several Ukrainian websites	O	CyberBerkut	DDoS (Passeri, 2015c)
23.12.2015	Ukrainian power grid	O/G	Unknown (probably Russian group)	BlackEnergy3 malware (Zetter, 2016)
01.2016	Kiev Boryspil Airport	O/G	Unknown (probably Russian group)	Similar to the malware from the power grid, probably BlackEnergy3 (Bolton, 2016; Polityuk and Prentice, 2016)
02.2016	Bellingcat website and email from a Bellingcat journalist	O	CyberBerkut	Defacement and leak of document stolen from the journalist's email account (Ashok, 2016; Crowdstrike, 2016, p. 5)
06.05.2016	Emails of Boris Dobrodeev, former boss of the Russian social network, vKontakte	O	Anonymous	Data breach and leak (Passeri, 2016)
05.2016	Alleged pro-Russian Ukrainian journalists	M	Myrotvorets a Ukrainian nationalist hacker group	Data breach and leak (Cimpanu, 2016)

Date	Victim	Type of victim	Alleged perpetrator	Technique/Tool
07.2016	20 Russian organizations (governmental, scientific and defense institutions)	G	Unknown	Unspecified malware (BBC News, 2016c)
07.2016	Ukrainian artillery	G	APT28	Malicious application for Android and Apple smartphones that intercepts communications and gives away user locations (Crowdstrike, 2016).
24.08.2016	Ukrainian Ministry of Defense and Ukrainian National Guard's Twitter and Instagram accounts	G	Pro-Russian or Russian actor named SPRUT	Defacement of their Twitter and Instagram accounts (Starks, 2016).
08.2016	Alleged pro-Russian Ukrainian journalists	M	Myrotvorets a Ukrainian nationalist hacker group	Data breach and leak (Cimpanu, 2016)
25.10.2016	Surkov's emails	G	CyberHunta	"Special software" (Miller, 2016b)
11.2016	OSCE	IO	Allegedly APT28	Unspecified (BBC News, 2016b)
06-08.12.2016	Ukrainian Ministry of Finance	G	Unknown	DDoS attack simultaneous with a system breach (Zetter, 2017).
06-08.12.2016	Ukrainian State Treasury	G	Unknown	DDoS attack simultaneous with a system breach (Zetter, 2017)
13.12.2016	Ukraine Ministry of Defense	G	Unknown	DDoS (Reuters, 2016b)
14.12.2016	Ukrainian State Administration of Railway Transport	G	Unknown	DDoS attack simultaneous with a system breach (Zetter, 2017)
17.12.2016	Ukrainian power substation in Pivnichna near Kiev	O/G	Unknown	BlackEnergy3 malware (Goodin, 2017)

7 Glossary

Backdoor: Part of a software code allowing hackers to remotely access a computer without the user's knowledge (Ghernaouti-Hélie, 2013, p. 426).

Botnet: Network of infected computers which can be accessed remotely and controlled centrally in order to launch coordinated attacks (Ghernaouti-Hélie, 2013, p. 427).

Confidence Building Measures (CBMs): Various procedures that can be established to build trust and prevent escalation between state-actors (United Nations, n.d.).

Data breach: Event in which information of a sensitive nature is stolen from a network without the users' knowledge (TrendMicro, 2017).

Distributed Denial of Service (DDoS): Act of overwhelming a system with a large number of packets through the simultaneous use of infected computers (Ghernaouti-Hélie, 2013, p. 431).

Euromaidan movement: Literally “European Square”; a movement of protest in support of the European Union Association Treaty that was cancelled by former Ukrainian President Yanukovych (Chervonenko, 2013).

Hacktivism: use of hacking techniques for political or social activism (Ghernaouti-Hélie, 2013, p. 433).

Internet exchange point: facility that interconnects two or more independent internet networks in order to facilitate internet traffic (Internet eXchange Federation, n.d.).

Internet Protocol (IP) address: A numerical address assigned to each device that uses the internet communications protocol allowing computers to communicate with one another (Internet Corporation For Assigned Names and Numbers, 2016).

Firmware: A software program programmed on a hardware device providing the instructions for communication between the device and other hardware. Firmware is stored in the flash read-only memory of the device (TechTerms, 2016).

Malware: Malicious software that can take the form of a virus, a worm or a Trojan horse (Collins and McCombie, 2012).

Patriotic hacking: Sometimes also referred to as nationalistic hacking. A group of individuals originating from a specific state engage in cyberattacks in defense against actors that they perceive to be enemies of their country (Denning, 2011, p. 178).

Payload: The part of malware that causes harmful results (PCmag, 2016).

Proxy: In computing, an intermediate server acting in place of end-users. This allows users to communicate without direct connections. This is often used for greater safety and anonymity in cyberspace (Ghernaouti-Hélie, 2013, p. 438).

Remote Administration or Access Tool (RAT): Software giving remote access and control to a computer without having physical access to it. RAT can be legitimate software, but also malicious (Siciliano, 2015).

Rootkit: Program downloading itself to an infected system and taking control of certain functions (Lindsay, 2013).

Spear phishing: A sophisticated phishing technique that not only imitates legitimate webpages, but also selects potential targets and adapts malicious emails to them. Emails often look like they come from a colleague or a legitimate company (Ghernaouti-Hélie, 2013, p. 440).

SQL Injection: A cyberattack technique in which malicious code to be executed by a SQL server is injected into code lines (Microsoft, 2016).

Supervisory Control And Data Acquisition (SCADA): Computer programs used to control industrial processes (Langner, 2013, p. 9).

Troll: A person submitting provocative statements or articles to an internet discussion in order to create discord and drag more people into it (Williams, 2012).

Troll farm or factory: Place running round the clock to produce trolling messages and posts (Volchek and Sindelar, 2015).

Watering hole attack: Attack where a legitimate website is injected with malicious code that redirects users to a compromised website which infects users accessing it (TechTarget, 2015).

Website defacement: Cyberattack replacing website pages or elements by other pages or elements (Ghernaouti-Hélie, 2013, p. 442).

Worm: Standalone, self-replicating program infecting and spreading to other computers through networks (Collins and McCombie, 2012).

8 Abbreviations

CBMs	Confidence Building Measures
CEC	Ukrainian Central Election Commission
CCDOE	NATO Cooperative Cyber Defence Centre of Excellence
DDoS	Distributed Denial of Service
EU	European Union
EW	Electronic Warfare
FSB	Federal Security Service - Russia
GRU	Main Intelligence Directorate - Russia
ICT	Information and Communications Technologies
IP	Internet Protocol
NATO	North Atlantic Treaty Organization
OSCE	Organization for Security and Co-operation in Europe
RAT	Remote Administration Tool
SCADA	Supervisory Control And Data Acquisition
SQL	Search Query Language

9 Bibliography

Ashok, I., 2016. Journalists investigating MH17 hacked by Russia-backed Fancy Bear hackers - ThreatConnect [WWW Document]. Int. Bus. Times. URL http://www.ibtimes.co.uk/journalists-investigating-mh17-hacked-by-russia-backed-fancy-bear-hackers-threatconnect-1583881 (accessed 08.02.17).

BanffCyber Technologies, 2016. Business Implications of Web Defacement [WWW Document]. BanffCyber Technol. URL https://www.banffcyber.com/business-implications-of-web-defacement/ (accessed 24.01.17).

BBC News, 2017. Ukraine conflict: Deadly flare-up in east [WWW Document]. BBC News. URL http://www.bbc.com/news/world-europe-38794679 (accessed 07.02.17).

BBC News, 2016a. Ukraine tests missiles near Crimea despite Russian ire [WWW Document]. BBC News. URL http://www.bbc.com/news/world-europe-38166597 (accessed 05.12.16).

BBC News, 2016b. OSCE security monitors targeted by hackers [WWW Document]. BBC News. URL http://www.bbc.com/news/world-europe-38451064 (accessed 05.01.17).

BBC News, 2016c. Russia cyber attack: Large hack “hits government” [WWW Document]. BBC News. URL http://www.bbc.com/news/world-europe-36933239 (accessed 31.10.16).

BBC News, 2014. Ukraine crisis: Timeline [WWW Document]. BBC News. URL http://www.bbc.com/news/world-middle-east-26248275 (accessed 22.11.16).

BBC News, 2006. Ukraine gas row hits EU supplies [WWW Document]. BBC News. URL http://news.bbc.co.uk/2/hi/europe/4573572.stm (accessed 22.11.16).

Bejtlich, R., 2015. Strategic Defence in Cyberspace: Beyond Tools and Tactics, in: Cyber War in Perspective: Russian Aggression against Ukraine. Kenneth Geers, Tallinn, pp. 159–170.

Besemeres, J., 2014. Russian disinformation and Western misconceptions [WWW Document]. Story. URL http://insidestory.org.au/russian-disinformation-and-western-misconceptions (accessed 17.11.16).

Bolton, D., 2016. Ukraine says major cyberattack on Kiev’s Boryspil airport was launched from Russia [WWW Document]. Independent. URL http://www.independent.co.uk/news/world/europe/ukraine-cyberattack-boryspil-airport-kiev-russia-hack-a6818991.html (accessed 19.01.17).

Brake, B., 2015. Strategic risks of ambiguity in cyberspace. Contigency Plan. Memo. 11.

Carr, J., 2014. Rival hackers fighting proxy war over Crimea [WWW Document]. CNN. URL http://edition.cnn.com/2014/03/25/opinion/crimea-cyber-war/ (accessed 18.11.16).

Chervonenko, V., 2013. Ukraine's EU options "still open" [WWW Document]. BBC News. URL http://www.bbc.com/news/world-europe-25087160 (accessed 06.12.16).

Cimpanu, C., 2016. Pro-Ukraine Hackers Leak Personal Details of Ukrainian and Foreign Journalists [WWW Document]. Softpedia. URL http://news.softpedia.com/news/pro-ukraine-hackers-leak-personal-details-of-ukrainian-and-foreign-journalists-507926.shtml (accessed 28.03.17).

Collins, S., McCombie, S., 2012. Stuxnet: the emergence of a new cyber weapon and its implications. J. Polic. Intell. Count. Terror. 7, 80–91. https://doi.org/10.1080/18335330.2012.653198

Crowdstrike, 2016. Use of Fancy Bear Android malware in tracking of Ukrainian field artillery units.

Denning, D.E., 2011. Cyber Conflict as an Emergent Social Phenomenon, in: Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications. Holt and Schell, pp. 170–186.

E-ISAC, 2016. Analysis of the Cyber Attack on the Ukrainian Power Grid. Electricity Information Sharing and Analysis Center, Washington, DC.

Emmott, R., 2016. Sanctions impact on Russia to be longer term, U.S. says [WWW Document]. Reuters. URL http://www.reuters.com/article/us-ukraine-crisis-sanctions-idUSKCN0UQ1ML20160112 (accessed 26.01.17).

European Union, 2015. Questions and Answers about the East StratCom Task Force [WWW Document]. Eur. Union Extern. Actions. URL http://collections.internetmemory.org/haeu/content/20160313172652/http://eeas.europa.eu/top_stories/2015/261115_stratcom-east_qanda_en.htm (accessed 27.03.17).

Farrell, H., 2015. Promoting Norms for Cyberspace [WWW Document]. Counc. Foreign Relat. URL http://www.cfr.org/cybersecurity/promoting-norms-cyberspace/p36358 (accessed 18.01.17).

FireEye Inc., 2016. FireEye Industry Intelligence Report cyber attacks on the Ukrainian grid: what you should know. FireEye Inc., Milpitas, CA.

FireEye Inc., 2015. HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group [WWW Document]. FireEye. URL https://www.fireeye.com/blog/threat-research/2015/07/hammertoss_stealthy.html (accessed 06.12.16).

Fiscutean, A., 2015. Cyber war in Ukraine: How NATO is helping the country defend itself against digital threats [WWW Document]. ZDNet Eur. URL http://www.zdnet.com/article/ukraines-cyber-warfare-how-nato-helps-the-country-defend-itself-against-digital-threats/ (accessed 17.11.16).

Foxall, A., 2016. Putin's Cyberwar: Russia's Statecraft in the Fifth Domain.

F-Secure, 2014. BLACKENERGY & QUEDAGH The convergence of crimeware and APT attacks. F-Secure, Helsinki.

Geers, K., 2015. Cyber war in perspective: Russian aggression against Ukraine. Tallinn.

Geers, K., 2014. Strategic Analysis: As Russia-Ukraine Conflict Continues, Malware Activity Rises [WWW Document]. FireEye. URL https://www.fireeye.com/blog/threat-research/2014/05/strategic-analysis-as-russia-ukraine-conflict-continues-malware-activity-rises.html (accessed 17.11.16).

Ghernaouti-Hélie, S., 2013. Cyberpower: crime, conflict and security in cyberspace, 1. ed. ed, Forensic sciences. EPFL Press, Lausanne.

Giles, K., 2016a. Russia's "new" tools for confronting the West: continuity and innovation in Moscow's exercise of power. Chatham House, London.

Giles, K., 2016b. The Next Phase Of Russian Information Warfare. NATO Strategic Communication Centre of Excellence, Riga, Latvia.

Giles, K., 2015. Russia and Its Neighbours: Old Attitudes, New Capabilities, in: Cyber War in Perspective: Russian Aggression against Ukraine. Kenneth Geers, Tallinn, pp. 19–28.

Giles, K., 2012. Russia's Public Stance on Cyberspace Issues, in: 2012 4th International Conference on Cyber Conflict (CYCON 2012): Tallinn, Estonia, 5 - 8 June 2012. IEEE, Piscataway, NJ, pp. 63–76.

Goodin, D., 2017. Hackers trigger yet another power outage in Ukraine [WWW Document]. Ars Tech. URL http://arstechnica.com/security/2017/01/the-new-normal-yet-another-hacker-caused-power-outage-hits-ukraine/ (accessed 19.01.17).

Gordon, M.R., 2014. NATO Commander Says He Sees Potent Threat From Russia [WWW Document]. N. Y. Times. URL http://www.nytimes.com/2014/04/03/world/europe/nato-general-says-russian-force-poised-to-invade-ukraine.html (accessed 18.11.16).

Gould, J., 2015. Electronic Warfare: What US Army Can Learn From Ukraine [WWW Document]. DefenseNews. URL http://www.defensenews.com/story/defense/

policy-budget/warfare/2015/08/02/us-army-ukraine-russia-electronic-warfare/30913397/ (accessed 17.08.16).

Gros, D., Mustilli, F., 2016. The Effects of Sanctions and Counter-Sanctions on EU-Russian Trade Flows [WWW Document]. Cent. Eur. Policy Stud. URL https://www.ceps.eu/publications/effects-sanctions-and-counter-sanctions-eu-russian-trade-flows (accessed 26.01.17).

Hackett, R., 2015. Russian cyberwar advances military interests in Ukraine, report says [WWW Document]. Fortune. URL http://fortune.com/2015/04/29/russian-cyberwar-ukraine/ (accessed 17.11.16).

Harding, L., 2016. Flight MH17 investigators to pinpoint missile launch in rebel-held Ukraine [WWW Document]. The Guardian. URL https://www.theguardian.com/world/2016/sep/27/mh17-inquiry-missile-launch-buk-ukraine-russia (accessed 28.11.16).

Hartog, E., 2016. A Kremlin Youth Movement Goes Rogue [WWW Document]. Mosc. Times. URL https://themoscowtimes.com/articles/a-kremlin-youth-movement-goes-rogue-52435 (accessed 28.11.16).

InfoSecurity, 2014. Snake Cyber-espionage Campaign Targetting Ukraine is Linked to Russia [WWW Document]. Infosecurity. URL http://www.infosecurity-magazine.com/news/snake-cyber-espionage-campaign-targetting-ukraine/ (accessed 18.11.16).

Internet Corporation For Assigned Names and Numbers, 2016. Glossary [WWW Document]. ICANN. URL https://www.icann.org/resources/pages/glossary-2014-02-03-en#i (accessed 04.11.16).

Internet eXchange Federation, n.d. Definition of an Internet Exchange Point [WWW Document]. IX-FInternet Exch. Fed. URL http://www.ix-f.net/ixp-definition.html (accessed 12.12.16).

Johnstone, L., 2014. #OpIndependence. Vitali Klitschko's UDAR party hacked. Confidential data leaked [WWW Document]. Cyberwarnews. URL https://www.cyberwarnews.info/2014/02/14/opindependence-vitali-klitschkos-udar-party-hacked-confidential-data-leaked/ (accessed 20.01.17).

Johnstone, L., 2013. Anonymous leak Ukraine Government Emails And Credentials for #OpUkraine [WWW Document]. Cyberwarnews. URL https://www.cyberwarnews.info/2013/12/28/anonymous-leak-ukraine-government-emails-and-credentials-for-opukraine/ (accessed 20.01.17).

Karmanau, Y., Isachenkov, V., 2014. Vladimir Putin admits for first time Russian troops took over Crimea, refuses to rule out intervention in Donetsk [WWW Document]. Natl. Post. URL http://news.nationalpost.com/news/world/vladimir-putin-admits-for-first-time-russian-troops-took-over-crimea-refuses-to-rule-out-intervention-in-donetsk (accessed 18.11.16).

Kenig, R., 2013. How Much Can a DDoS Attack Cost Your Business? [WWW Document]. Radware Blog. URL https://blog.radware.com/security/2013/05/how-much-can-a-ddos-attack-cost-your-business/ (accessed 23.01.17).

Kerkkänen, T., Kuronen, A., 2016. Russia's Cyberwar in Ukraine is Relentless – This Hacktivist Strikes Back [WWW Document]. YLE. URL http://yle.fi/uutiset/osasto/news/russias_cyberwar_in_ukraine_is_relentless__this_hacktivist_strikes_back/8918200 (accessed 02.12.16).

Kovacs, E., 2014. Website of International Video News Agency Ruptly Hit With DDOS Attack [WWW Document]. Softpedia. URL http://news.softpedia.com/news/Website-of-International-Video-News-Agency-Ruptly-Hit-With-DDOS-Attack-430390.shtml (accessed 20.01.17).

Kovacs, E., 2013a. Ukraine's State Customs Service Targeted by Anonymous Hackers [WWW Document]. Softpedia. URL http://news.softpedia.com/news/Ukraine-s-State-Customs-Service-Targeted-by-Anonymous-Hackers-400518.shtml (accessed 20.01.17).

Kovacs, E., 2013b. Government Website of Ukraine's Brovary Region Hacked [WWW Document]. Softpedia. URL http://news.softpedia.com/news/Government-Website-of-Ukraine-s-Brovary-Region-Hacked-407646.shtml (accessed 20.01.17).

Koval, N., 2015. Revolution Hacking, in: Cyber War in Perspective: Russian Aggression against Ukraine. Kenneth Geers, Tallinn, pp. 55–58.

Lally, K., Englund, W., Booth, W., 2014. Russian parliament approves use of troops in Ukraine [WWW Document]. Wash. Post. URL https://www.washingtonpost.com/world/europe/russian-parliament-approves-use-of-troops-in-crimea/2014/03/01/d1775f70-a151-11e3-a050-dc3322a94fa7_story.html (accessed 22.11.16).

Lange-Ionatamishvili, E., Svetoka, S., 2015. Strategic Communications and Social Media in the Russia Ukraine Conflict, in: Cyber War in Perspective: Russian Aggression against Ukraine. Kenneth Geers, Tallinn, pp. 103–112.

Langner, R., 2013. To kill a centrifuge: a technical analysis of what Stuxnet's creators tried to achieve.

Lewis, J.A., 2015. 'Compelling Opponents to Our Will': The Role of Cyber Warfare in Ukraine, in: Cyber War in Perspective: Russian Aggression against Ukraine. Kenneth Geers, Tallinn, pp. 39–47.

Libicki, M.C., 2015. The Cyber War that Wasn't, in: Cyber War in Perspective: Russian Aggression against Ukraine. Kenneth Geers, Tallinn, pp. 49–54.

Lin, H., 2012. Escalation Dynamics and Conflict Termination in Cyberspace. Strateg. Stud. Q. 6, 46–70.

Lindsay, J.R., 2013. Stuxnet and the Limits of Cyber Warfare. Secur. Stud. 22, 365–404. https://doi.org/10.1080/09636412.2013.816122

Maheshwari, V., 2015. Ukraine's Lonely Cyberwarrior vs. Russia [WWW Document]. Dly. Beast. URL http://www.thedailybeast.com/articles/2015/02/18/ukraine-s-lonely-cyber-warrior.html (accessed 05.12.16).

Martin-Vegue, T., 2015. Are we witnessing a cyber war between Russia and Ukraine? Don't blink - you might miss it [WWW Document]. CSOonline.com. URL http://www.csoonline.com/article/2913743/cyber-attacks-espionage/are-we-witnessing-a-cyber-war-between-russia-and-ukraine-dont-blink-you-might-miss-it.html (accessed 17.11.16).

Maurer, T., 2015. Cyber Proxies and the Crisis in Ukraine, in: Cyber War in Perspective: Russian Aggression against Ukraine. Kenneth Geers, Tallinn, pp. 79–86.

Microsoft, 2016. SQL Injection [WWW Document]. Microsoft TechNet. URL https://technet.microsoft.com/en-us/library/ms161953(v=SQL.105).aspx (accessed 29.11.16).

Miller, C., 2016a. Ukraine Searches For Culprit After Cyberattacks On Finance Ministry, Treasury [WWW Document]. RadioFreeEurope RadioLiberty. URL http://www.rferl.org/a/ukraine-cyberattacks-finance-ministry-treasury-infrastructure-russia/28172004.html (accessed 20.01.17).

Miller, C., 2016b. Inside The Ukrainian "Hacktivist" Network Cyberbattling The Kremlin [WWW Document]. RadioFreeEurope RadioLiberty. URL http://www.rferl.org/a/ukraine-hacktivist-network-cyberwar-on-kremlin/28091216.html (accessed 03.11.16).

Nocetti, J., 2015. Guerre de l'information : le web russe dans le conflit en Ukraine. Focus Strat. 62, 1–47.

NSFocus Inc., 2016. Distributed Denial-of-Service (DDoS) Attacks: An Economic Perspective (Whitepaper). NSFocus Inc., Santa Clara, CA.

Paganini, P., 2014a. BAE Systems Applied Intelligence has disclosed a Russian cyber espionage campaign codenamed as SNAKE that targeted Governments and Military Networks [WWW Document]. Secur. Aff. URL http://securityaffairs.co/wordpress/22875/intelligence/snake-cyber-espionage-campaign.html (accessed 28.11.16).

Paganini, P., 2014b. Crimea – The Russian Cyber Strategy to Hit Ukraine [WWW Document]. Infosec Inst. URL http://resources.infosecinstitute.com/crimea-russian-cyber-strategy-hit-ukraine/ (accessed 18.11.16).

Pakharenko, G., 2015. Cyber Operations at Maidan: A First-Hand Account, in: Cyber War in Perspective: Russian Aggression against Ukraine. Kenneth Geers, Tallinn, pp. 59–66.

Paladion Networks, 2015. Website Defacement: Costs and Prevention [WWW Document]. Paladion. URL http://paladion.net/website-defacement-costs-and-prevention/ (accessed 24.01.17).

Passeri, P., 2016. 1-15 May 2016 Cyber Attacks Timeline [WWW Document]. HACKMAGEDDON. URL http://www.hackmageddon.com/2016/06/08/1-15-may-2016-cyber-attacks-timeline/ (accessed 28.03.17).

Passeri, P., 2015a. 1-15 January 2015 Cyber Attacks Timeline [WWW Document]. HACKMAGEDDON. URL http://www.hackmageddon.com/2015/01/20/1-15-january-2015-cyber-attacks-timeline/ (accessed 28.03.17).

Passeri, P., 2015b. 16-28 February 2015 Cyber Attacks Timeline [WWW Document]. HACKMAGEDDON. URL http://www.hackmageddon.com/2015/03/01/16-28-february-2015-cyber-attacks-timeline/ (accessed 28.03.17).

Passeri, P., 2015c. 16-31 August 2015 Cyber Attacks Timeline [WWW Document]. HACKMAGEDDON. URL http://www.hackmageddon.com/2015/09/07/16-31-august-2015-cyber-attacks-timeline/ (accessed 28.03.17).

Passeri, P., 2014a. 16-31 March 2014 Cyber Attacks Timeline [WWW Document]. HACKMAGEDDON. URL http://www.hackmageddon.com/2014/04/14/16-31-march-2014-cyber-attacks-timeline/ (accessed 28.03.17).

Passeri, P., 2014b. 16-31 July 2014 Cyber Attacks Timeline [WWW Document]. HACKMAGEDDON. URL http://www.hackmageddon.com/2014/08/05/16-31-july-2014-cyber-attacks-timeline/ (accessed 28.03.17).

Passeri, P., 2014c. 1-15 August 2014 Cyber Attacks Timeline [WWW Document]. HACKMAGEDDON. URL http://www.hackmageddon.com/2014/08/19/1-15-august-2014-cyber-attacks-timeline/ (accessed 28.03.17).

Paul, C., Matthews, M., 2016. The Russian “Firehose of Falsehood” Propaganda Model: Why It Might Work and Options to Counter It (No. PE-198-OSD), Perspectives. RAND Corporation, Santa Monica, CA.

PCmag, 2016. Definition of: payload [WWW Document]. PCmag. URL http://www.pcmag.com/encyclopedia/term/48909/payload (accessed 12.12.16).

Perlroth, N., 2014. Cyberattacks Rise as Ukraine Crisis Spills to Internet [WWW Document]. N. Y. Times. URL http://bits.blogs.nytimes.com/2014/03/04/cyberattacks-rise-as-ukraine-crisis-spills-on-the-internet/ (accessed 18.11.16).

Polityuk, P., Prentice, A., 2016. Ukraine says to review cyber defenses after airport targeted from Russia [WWW Document]. Reuters. URL http://www.reuters.com/article/us-ukraine-cybersecurity-malware-idUSKCN0UW0R0 (accessed 19.01.17).

Poludenko-Young, A., 2015. Dear Ukrainian Officials: Russian Security Services Thank You for Your Cooperation! [WWW Document]. Glob. Voices Online. URL https://globalvoices.org/2015/05/23/ukrainian-officials-russian-security-services-thank-you-for-your-cooperation/ (accessed 17.11.16).

Reuters, 2016a. Russia Withdraws Backing for International Criminal Court Treaty [WWW Document]. N. Y. Times. URL http://www.nytimes.com/reuters/2016/11/16/world/europe/16reuters-russia-icc-withdrawal.html?ref=world&_r=0 (accessed 22.11.16).

Reuters, 2016b. Ukraine’s defence ministry says website hit by cyber attack [WWW Document]. Reuters. URL http://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN1421YT (accessed 24.01.17).

Sanger, D.E., Erlanger, S., 2014. Suspicion Falls on Russia as ‘Snake’ Cyberattacks Target Ukraine’s Government [WWW Document]. N. Y. Times. URL http://www.nytimes.com/2014/03/09/world/europe/suspicion-falls-on-russia-as-snake-cyberattacks-target-ukraines-government.html?_r=1 (accessed 18.11.16).

Selhorst, T., 2016. Russia’s Perception Warfare. Mil. Spect. 185, 148–164.

Shachtman, N., 2009. Kremlin Kids: We Launched the Estonian Cyber War [WWW Document]. Wired. URL https://www.wired.com/2009/03/pro-kremlin-gro/ (accessed 09.12.16).

Shahani, A., 2015. Report: To Aid Combat, Russia Wages Cyberwar Against Ukraine [WWW Document]. NPR. URL http://www.npr.org/sections/alltechconsidered/2015/04/28/402678116/report-to-aid-combat-russia-wages-cyberwar-against-ukraine (accessed 18.11.16).

Shevchenko, V., 2014. Ukraine conflict: Hackers take sides in virtual war [WWW Document]. BBC News. URL http://www.bbc.com/news/world-europe-30453069 (accessed 28.11.16).

Siciliano, R., 2015. What is a Remote Administration Tool (RAT)? [WWW Document]. McAfee Blog. URL https://securingtomorrow.mcafee.com/consumer/identity-protection/what-is-rat/ (accessed 04.11.16).

Standish, R., 2015. Does the Kremlin Have a New Way of Hacking the West? [WWW Document]. Foreign Policy. URL http://foreignpolicy.com/2015/07/29/does-the-kremlin-have-a-new-way-of-hacking-the-west-hammertoss-fireeye-apt29/ (accessed 08.12.16).

Starks, T., 2016. Russia’s cyberspace footprint gets bigger [WWW Document]. PoliticoMagazine. URL http://www.politico.com/tipsheets/morning-cybersecurity/2016/08/russias-cyberspace-footprint-gets-bigger-216075 (accessed 08.02.17).

Stauffacher, D., Kavanagh, C., 2013. Confidence Building Measures and International Cyber Security. ICT4Peace, Geneva, Switzerland.

Storm, D., 2014. Political hackers attack Russia, Nazi defacement, threaten US CENTCOM with cyberattack [WWW Document]. Computerworld. URL http://www.computerworld.com/article/2476002/cybercrime-hacking/political-hackers-attack-russia--nazi-defacement--threaten-us-centcom-with-cybera.html (accessed 23.11.16).

Stratfor, 2012. Russia: The fate of the Nashi Youth Movement [WWW Document]. Stratfor. URL https://www.stratfor.com/sample/analysis/russia-fate-nashi-youth-movement (accessed 29.11.16).

Symantec Security Response, 2014. Turla: Spying tool targets governments and diplomats [WWW Document]. Symantec. URL https://www.symantec.com/connect/blogs/turla-spying-tool-targets-governments-and-diplomats (accessed 23.11.16).

Tatham, S., 2015. The solution to Russian propaganda is not EU or NATO propaganda but advanced social science to understand and mitigate its effect in trageted population (No. 4), Policy Paper. National Defence Academy of Latvia - Center for Security and Strategic Research, Riga, Latvia.

TechTarget, 2015. watering hole attack [WWW Document]. TechTarget. URL http://searchsecurity.techtarget.com/definition/watering-hole-attack (accessed 29.11.16).

TechTerms, 2016. Firmware [WWW Document]. TechTerms. URL http://techterms.com/definition/firmware (accessed 08.12.16).

The Moscow Times, 2014. “Cyber Berkut” Hackers Target Major Ukrainian Bank [WWW Document]. Mosc. Times. URL https://themoscowtimes.com/articles/cyber-berkut-hackers-target-major-ukrainian-bank-37033 (accessed 22.11.14).

Thielman, S., Ackerman, S., 2016. Cozy Bear and Fancy Bear: did the Russians hack Democratic party and if so, why? [WWW Document]. The Guardian. URL https://www.theguardian.com/technology/2016/jul/29/cozy-bear-fancy-bear-russia-hack-dnc (accessed 25.10.16).

Torruella, R.A., 2014. Determining Hostile Intent in Cyberspace. Jt. Force Q. 75 114–121.

TrendMicro, 2017. Definition [WWW Document]. TrendMicro. URL http://www.trendmicro.com/vinfo/us/security/definition/data-breach (accessed 17.01.17).

Tucker, P., 2014. Why Ukraine Has Already Lost The Cyberwar, Too [WWW Document]. Def. One. URL http://www.defenseone.com/technology/2014/04/why-ukraine-has-already-lost-cyberwar-too/83350/ (accessed 17.11.16).

Ukraine investigations, 2014. Cyber Wars: The Invisible Front [WWW Document]. Ukr. Investig. URL http://ukraineinvestigation.com/cyber-wars-invisible-front/ (accessed 17.11.16).

United Nations, 1994. Memorandum on Security Assurances in Connection with Ukraine’s Accession to the Treaty on the Non-Proliferation of Nuclear Weapons.

United Nations, n.d. Military Confidence-building [WWW Document]. U. N. Off. Disarm. Aff. URL https://www.un.org/disarmament/cbms/ (accessed 16.03.17).

Volchek, D., Sindelar, D., 2015. One Professional Russian Troll Tells All [WWW Document]. RadioFreeEurope RadioLiberty. URL http://www.rferl.org/a/how-to-guide-russian-trolling-trolls/26919999.html (accessed 22.11.16).

Walker, S., Rankin, J., 2014. Western food imports off the menu as Russia hits back over Ukraine sanctions [WWW Document]. The Guardian. URL https://www.theguardian.com/world/2014/aug/07/russia-bans-western-food-imports-retaliation-ukraine-sanctions (accessed 22.11.16).

Waqas, A., 2014. 30 Ukrainian government and media websites defaced by neo-fascist Svoboda party [WWW Document]. HackRead. URL https://www.hackread.com/ukrainian-government-websites-hacked-by-new-nazi-hackers/ (accessed 20.01.17).

Weaver, M., Luhn, A., 2015. Ukraine ceasefire agreed at Belarus talks [WWW Document]. The Guardian. URL https://www.theguardian.com/world/2015/feb/12/ukraine-crisis-reports-emerge-of-agreement-in-minsk-talks (accessed 22.11.16).

Weedon, J., 2015. Beyond ‘Cyber War’: Russia’s Use of Strategic Cyber Espionage and Information Operations in Ukraine, in: Cyber War in Perspective: Russian Aggression against Ukraine. Kenneth Geers, Tallinn, pp. 67–77.

What Effect Will U.S. Sanctions Have On Russia?, 2016. . Things Consid.

White, G.L., 2014. Russia’s Putin Signs Treaty to Annex Crimea [WWW Document]. Wall Str. J. URL http://www.wsj.com/articles/SB10001424052702304747404579446920731715270 (accessed 22.11.16).

Williams, Z., 2012. What is an internet troll? [WWW Document]. The Guardian. URL https://www.theguardian.com/technology/2012/jun/12/what-is-an-internet-troll (accessed 05.12.16).

Windrew, R., 2016. Payback? Russia gets hacked, revealing Putin aide’s secrets [WWW Document]. CNBC. URL http://www.cnbc.com/2016/10/28/payback-russia-gets-hacked-revealing-putin-aides-secrets.html (accessed 03.11.16).

Witty, R., 2015. LookingGlass Cyber Threat Intelligence Group Links Russia to Cyber Espionage Campaign Targeting Ukrainian Government and Military Officials [WWW Document]. LookingGlass. URL https://www.lookingglasscyber.com/press-release/lookingglass-cyber-threat-intelligence-group-links-russia-to-cyber-espionage-campaign-targeting-ukrainian-government-and-military-officials/ (accessed 28.11.16).

Zetter, K., 2017. The Ukrainian Power Grid Was Hacked Again [WWW Document]. Motherboard. URL http://motherboard.vice.com/read/ukrainian-power-station-hacking-december-2016-report (accessed 19.01.17).

Zetter, K., 2016. Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid [WWW Document]. Wired. URL https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ (accessed 23.11.16).

Zetter, K., 2014. Russian ‘Sandworm’ Hack Has Been Spying on Foreign Governments for Years [WWW Document]. Wired. URL https://www.wired.com/2014/10/russian-sandworm-hack-isight/ (accessed 29.11.16).

CSS CYBER DEFENSE PROJECT

Hotspot Analysis:

Addendum to Cyber and Information warfare in the Ukrainian conflict

Zürich, October 2018

Addendum 1

Risk and Resilience Team
Center for Security Studies (CSS), ETH Zürich

Author: Marie Baezner

Contact:
Center for Security Studies
Haldeneggsteig 4
ETH Zürich
CH-8092 Zürich
Switzerland
Tel.: +41-44-632 40 25
css@sipo.gess.ethz.ch
www.css.ethz.ch

Analysis prepared by: Center for Security Studies (CSS), ETH Zürich

ETH-CSS project management: Tim Prior, Head of the Risk and Resilience Research Group; Myriam Dunn Cavelty, Deputy Head for Research and Teaching; Andreas Wenger, Director of the CSS

Disclaimer: The opinions presented in this study exclusively reflect the authors' views.

Please cite as: Baezner, Marie (2018): Addendum to Cyber and Information warfare in the Ukrainian conflict, October 2018, Center for Security Studies (CSS), ETH Zürich.

Table of Contents

1 Introduction

In 2017 and 2018, the cyber-dimension of the Ukrainian conflict continued to attract attention. The conflict between pro-Russian separatists and the Ukrainian government in East Ukraine is ongoing and cybermeans still play an important strategic role in the conflict.

This addendum is meant to be read as a complement to the Hotspot Analysis on Cyber and Information warfare in the Ukrainian conflict. Hotspot Analyses are meant to be updated when new information or events occur to keep them as up-to-date as possible. Since the June 2017 publication of the Hotspot Analysis on Cyber and Information warfare in the Ukrainian conflict, several important incidents occurred in the Ukrainian cybersphere. First, reports revealing new information regarding the cyberattack on the Ukrainian power grid in December 2016 were published. Second, Ukraine fell victim to significant ransomware[1] attacks (e.g. NotPetya and BadRabbit). Third, low-level cyberattacks like Distributed Denial of Service (DDoS)[2] attacks and website defacements continued to be used regularly. Fourth, in May 2018, a major malware infection of routers specifically targeting Ukraine was uncovered.

This addendum aims to analyze these new cyber-events in Ukraine and help provide a more complete Hotspot Analysis. The addendum to the Hotspot Analysis on Cyber and Information warfare in the Ukrainian conflict is structured as follows: Section 2 explores the context in which the new cyberattacks occurred. A chronology helps to understand the proceedings of events in Ukraine since January 2017. Section 3 describes the new malware found in Ukraine and their functionalities. The section also gives some additional details on two actors believed to be behind high-profile cyberattacks in Ukraine. Section 4 analyzes the domestic effects of the recent cyberattacks on society, the economy, and technology, as well as the effect on international relations. Finally, Section 5 provides some general recommendations for other states to mitigate the risks of succumbing to similar cyberattacks as in Ukraine.

2 Background and chronology

Since January 2017, the conflict in Ukraine has persisted in the physical and cyber realms. In this period, Ukraine was significantly affected by large-scale cyberattacks attributed to Russian actors. Simultaneously, Ukraine also attempted to build closer ties with the West by starting discussions on a potential NATO membership. The following chronology provides a timeline of relevant events.

Rows with a gray background refer to cyber-related incidents.

Date	Event
03.2017	Sandworm infiltrates a Ukrainian software company to gain access to Ukrainian financial institutions' networks (Cherepanov, 2017a).
16.05.2017	The Ukrainian President decides to ban several Russian social network and media websites. After the announcement, his personal website is taken down by a cyberattack (BBC News, 2017a; Luhn, 2017).
20.06.2017	The US broadens its sanctions against Russia (Walker and Borger, 2017).
27.06.2017	A cyberattack hits Ukrainian critical infrastructure and spreads worldwide. The malware, known as NotPetya, poses as a ransomware. In reality, the data encrypted by the malware cannot be decrypted; researchers believe that the attackers' intent with NotPetya was to cause damage and not generate revenue (Cherepanov, 2017a).
10.07.2017	The Ukrainian President meets with the Secretary General of NATO to discuss an action plan for Ukraine to become a NATO member (BBC News, 2017b).
12.07.2017	NATO members agree to help Ukraine with expertise and equipment in the investigation into NotPetya (Paganini, 2017a).
14-20.09.2017	Russia and Belarus conduct a significant joint military exercise near their Eastern border (Marcus, 2017).

[1] Technical terms are explained in a glossary in section 7

[2] Abbreviations are listed in Section 8.

29.09.2017	Ukraine and the US hold their first Bilateral Cyber Dialogue. The US agrees to give US$5 million to Ukraine to strengthen its defensive cyber capabilities (US Embassy Kyiv, 2017).
24.10.2017	The ransomware BadRabbit infects media outlets in Russia and infrastructure in Ukraine, before spreading to other countries (Hern, 2017a).
11.2017	The CIA attributes the NotPetya cyberattack to the Russian Main Intelligence Directorate (GRU) (Nakashima, 2018).
02.11.2017	Ukraine Security Services (SBU) accuses APT28 to be behind the BadRabbit malware (Bing, 2017).
27.12.2017	Ukraine and pro-Russian separatists exchange prisoners. It is the first exchange since the beginning of the conflict (Bennetts, 2017).
06.02.2018	The Ukrainian power distributor Ukrenergo declares an investment of US$20 million in a new cyberdefense system that will come into force in 2020 (Reuters Staff, 2018).
15.02.2018	The US, United Kingdom and Denmark officially attribute NotPetya to Russia (Geller, 2018).
03.05.2018	The US State Department announces that it will increase its aid to Ukraine for cybersecurity to US$10 million (Lyngaas, 2018).
23.05.2018	Cisco Talos publishes a blog report on VPNFilter, a malware infecting routers and Network-Attached Storage (NAS) devices. The publication follows numerous observations regarding the high rates of malware infection on Ukrainian devices (Largent, 2018a).
24.05.2018	The US Federal Bureau of Investigation (FBI) seizes a domain used by VPNFilter's operators as its Command and Control infrastructure (C&C), to stop a possibleattack on UKraine (Otto, 2018).
06.06.2018	Cisco Talos updates its blog report on VPNFilter and announces that the threat is more serious than previously thought (Largent, 2018b).
26.06.2018	Ukraine Cyber Police warns that Russian hackers have been planting backdoors in Ukrainian companies' networks in preparation for an upcoming large and highly coordinated cyberattack (Polityuk, 2018).

3 Description

Since January 2017, there have been a number of advancements in regard to tools, techniques, targets, and actors in Ukrainian cybersphere. In particular, new malware proved highly effective against Ukrainian targets, and significant information on actors in cyberspace was revealed.

3.1 Tools and techniques

While Ukrainian websites continue to suffer occasional DDoS attacks in this reporting period, the most significant technical developments included widespread ransomware, as well as new malware that infected high amounts of routers and connected devices.

DDoS

DDoS attacks have continued to affect Ukrainian websites. The new attacks target the websites of governmental institutions and are emblematic of the tit-for-tat cyberattacks between Moscow and Kiev. These attacks often follow influential or large-scale events in the ongoing conflict, or are in response to political events. DDoS attacks do not require sophisticated skills and are not particularly damaging to the target. Pro-Russian or anti-government hacktivists and patriotic hackers are often behind such attacks. These attacks usually serve to publicize the hacktivists' protests against the Ukrainian government.

Malware

Several sophisticated malware linked to the Ukrainian conflict have been observed since January 2017. The spread of the malware was largely contained to within Ukraine, but some had global ramifications. Five new malware have been identified since January 2017:

CrashOverride

CrashOverride[3] was the malware used to attack the Ukrainian power grid in December 2016. CrashOverride has a modular framework that enables it to adapt to its environment. The malware was not specifically designed for the Ukrainian power grid and can be easily reused against other industrial targets. CrashOverride is composed of a backdoor and several modules. It is designed to access the Industrial Control System (ICS) of its target remotely. The malware is designed without any function to exfiltrate data, which suggests that its objective is not cyberespionage, but to cause damage. One module works to remove data and overwrite the ICS configurations, rendering the ICS unusable. It is possible that the attack on the power grid in December 2016 was to test the malware. The cybersecurity firm Dragos Inc. attributed CrashOverride to Sandworm (Cherepanov, 2017b; Dragos Inc., 2017; Greenberg, 2017a).

NotPetya

NotPetya[4] is a worm that has the appearance of a ransomware. When in use, the worm distracted its targets from other cyberespionage campaigns and/or disruptive attacks. The malware spread throughout Ukraine, before infecting computers in other countries. In total, NotPetya infected approximately 17,000 computers worldwide of which 12,500 were Ukrainian (Palmer, 2017). Some of the code from NotPetya was taken from known ransomware, referred to as Petya, to make it look like the same tool. NotPetya also borrowed features from the WannaCry[5] ransomware, for example the use of the EternalBlue exploit (Hern, 2017b). Unlike the other ransomware tools, NotPetya encrypted the data it accessed in a way that it rendered it impossible to recover. This specific element led cybersecurity experts to conclude that NotPetya did not seek to gain financial advantage. The perpetrators infiltrated the servers of software that was widely used in the Ukrainian tax system, and injected the malware in the updates of the legitimate software to infect the users. The ransomware spread outside Ukraine through Virtual Private Networks (VPN). Cybersecurity experts attributed NotPetya to Sandworm. Before NotPetya, Ukraine was hit by three other malware that all took the appearance of known ransomware; two were pushed through the same tax filing software update server. It is very likely that these ransomware were designed and employed by Sandworm (Borys, 2017; Cherepanov, 2017a, 2017c; Cimpanu, 2017a, 2017b, 2017c).

BadRabbit

BadRabbit is a ransomware that started to spread widely throughout Russia and Ukraine in 2017 and the first half of 2018. The ransomware shares some similarities with NotPetya and WannaCry. BadRabbit infected its victims through a fake Adobe Flash update. Unlike NotPetya, BadRabbit decrypted the data once the ransom was paid. The SBU accused APT28 of

[3] CrashOverride is also known as Industroyer.

[4] NotPetya is also known as Diskcoder.C, ExPetr, PetrWrap and Petya.

[5] For more information on WannaCry, please see Baezner, Marie (2018): Hotspot Analysis: Cyber disruption and cybercrime: Democratic People's Republic of Korea, June 2018, Center for Security Studies (CSS), ETH Zürich.

perpetrating the BadRabbit attacks and of using the ransomware as a diversion while launching a phishing campaign. However, attribution is far from conclusive; the cybersecurity firm ESET attributed BadRabbit to Sandworm (BBC News, 2017c; Bing, 2017; Hern, 2017a; Mamedov et al., 2017).

VPNFilter

VPNFilter is a malware that infects routers and other connected devices like Network-Attached Storage (NAS). Talos, the Cyber Threat Alliance, and US law enforcement agencies revealed in May 2018 that VPNFilter has infiltrated more than 500,000 routers in 54 countries. The malware scans the internet for devices with vulnerabilities and then infects them. Routers are known to possess vulnerabilities and are difficult to patch and protect against threats. Many brands and models of routers are reported to be potentially affected by VPNFilter. The malware shares some strings of code with the BlackEnergy malware. Attackers can use the infected devices as a botnet; monitor internet traffic going through the infected devices; render single or groups of devices unusable by overwriting the firmware; conduct man-in-the-middle attacks by intercepting and tampering data going through the devices; and look for ICS communication traffic. VPNFilter also has a function that renders it persistent to reboots (most malware infecting connected devices do not survive a reboot), and therefore differentiates it from other malware that targets connected devices. In May 2018, Talos observed the malware was becoming increasingly targeting Ukrainian targets, and feared preparations for a significant coordinated cyberattack may be underway. The US Department of Justice attributed VPNFilter to APT28 and cybersecurity experts narrowed the perpetrator to Sandworm (Bing, 2018a; Largent, 2018b, 2018a; Otto, 2018; Symantec Security Response, 2018).

Python/TeleBot

Python/Telebot is a Trojan that targeted Ukrainian financial institutions in 2016. The malware spread through spear phishing emails with infected Excel documents. Python/TeleBot was sent in spear phishing emails from the same servers as the BlackEnergy malware used in the Ukrainian power grid attack of December 2015. Python/Telebot, notably, has the ability to communicate with the attackers and to receive commands through a Telegram Messenger chat. The malware can steal files, collect information on the computer, take screenshots and upload additional malware (Cherepanov, 2016).

3.2 Targets

Few significant developments regarding the primary targets of cyberattacks have been recorded since January 2017. Cyberattacks still largely target Ukrainian institutions and companies. However, the Ukrainian energy sector seems to remain a preferred choice of target.

3.3 Attribution and actors

Attribution in cyberspace stays a subject of contention. However, we observe that the past years states and cybersecurity firms tended to attribute cyberattacks more easily. Often, attribution follows the logic of *cui bono* (to whose benefit) and cases of cyberattacks in Ukraine conform to this pattern. In the case of Ukraine, attributing cyberattacks to Russia seems highly obvious. However, it is important to bear in mind that technical evidence could be used to incriminate a particular actor, if deliberately planted by the attackers to mislead the investigators. In addition, this addendum is mostly based on cybersecurity reports and media articles, which are written for a particular audience and may not be objective.

No new cyberactors have entered the scene of the Ukrainian conflict. Nevertheless, new information on familiar groups completes the descriptions provided by the Hotspot Analysis.

Pro-Russian hacker groups

Sandworm

Sandworm[6] was originally referred to as Quedagh in the Hotspot Analysis on Cyber and Information warfare in the Ukrainian conflict[7]. F-Secure suspects the group to have been active since at least 2008, and to have played a role in the conflict between Russia and Georgia. Sandworm has used different versions of the BlackEnergy toolkit since 2010 against both political and strategic targets. The group is patient and well-resourced. Sandworm develops its own cybertools and customizes them to be most effective against its targets (F-Secure, 2014, p. 4). Sandworm conducts significant campaigns in Ukraine; it is said to be a subunit of APT28, and therefore is associated with the Russian Main Intelligence Directorate (GRU). Various cybersecurity experts have attributed the most recent attacks in Ukraine - CrashOverride, Python/TeleBot, NotPetya, BadRabbit and VPNFilter - to the group (Bing, 2018b; Cherepanov, 2017c, 2017b; Dragos Inc., 2017; Greenberg, 2017b).

[6] Sandworm is also known as Quedagh, Voodoo Bear, TeleBots, BlackEnergy group.

[7] In the research for the addendum, it came to attention that Quedagh and Sandworm were the same group. Therefore, it was decided to use the group's most common name in the addendum.

Gamaredon Group

The Gamaredon Group is believed to be the 16th and 18th Centers of the Russian Federal Security Service (FSB). Cybersecurity experts have attributed Operation Armageddon to the group; that cyberattack has targeted the Ukrainian government, military and law enforcement since 2014. The Gamaredon Group typically employs spear phishing emails with malicious documents attached to infect its targets. The group is known to use publicly available cybertools but has recently improved its technical capabilities and has begun develop its own tailored malware (Kasza and Reichel, 2017; Paganini, 2017b).

4 Effects

This section analyses the effects of cyberattacks against Ukrainian targets on society, the economy, technology and international relations since January 2017.

4.1 Social and political effects

Since January 2017, the social and political ramifications of continuing cyberattacks in the Ukrainian conflict were limited. Ukraine further developed its defensive cyber capabilities and published a national cybersecurity strategy. Ukrainian authorities also attempted to counter pro-Russian propaganda by blocking Russian social media. Despite the government's attempts, such reforms have not engendered in Ukrainian society a greater level of confidence in their own security.

Ukraine develops its cyber capabilities

Since the beginning of the conflict, Ukraine has worked to bolster its cyber capabilities. Before the outbreak of war, Ukraine's cyber capabilities were limited. The conflict also unintentionally served to highlight the importance of the cyber-dimension to Ukrainian authorities. With some international support, Ukraine developed its cyberdefense capabilities and published a national cybersecurity strategy in 2016 (Brantly et al., 2017). The leading authority on cybersecurity in Ukraine is the Security Services (SBU) a civilian law enforcement agency that also concentrates most of cybersecurity resources. On the one side, having the SBU as lead for cybersecurity issues in Ukraine indicates a focus on fighting cybercrime from the Ukrainian authorities. On the other side, Ukrainian troops are regularly targeted by cyber-operations from pro-Russian groups that the Ukrainian military cyberdefense unit cannot fight effectively due to a lack of resources. This imbalance in resources between the civilian and military cybersecurity entities is surprising for a country that is at war. The SBU argues that cyberattacks against Ukrainian institutions (including military) are part of Russian hybrid warfare strategy and that hostile actions in East Ukraine are acts of terrorism. Therefore, the SBU concluded that a civilian-centric approach to cyberattacks is justified (Brantly et al., 2017).

Ukraine government blocking Russian websites

Ukrainian authorities tried to limit Russian campaigns to influence social media by blocking Russian social media websites because many Ukrainians use Russian-based social media platforms such as VKontakte. Throughout the Ukrainian conflict, pro-

Russian separatists have exploited social media to harass and collect data on Ukrainian soldiers and their families, and to spread messages of propaganda (Brantly et al., 2017). In May 2017, the Ukrainian president decided to sanction these websites and to block them in Ukraine for three years (Luhn, 2017). This policy proved highly unpopular, and the Ukrainian president's website was taken down by a cyberattack allegedly originating from Russia (BBC News, 2017a). This event demonstrates how little the situation in cyberspace has changed since January 2017. Tit-for-tat cyberattacks between warring parties continue to thrive. However, it is important to note that Ukrainian authorities are not only aware of, but also try to actively counter, pro-Russian influence campaigns on social media. Nevertheless, banning websites will not solve the problem. To counter such a pervasive problem, the effort needs to come from the whole society.

Recurrent feeling of insecurity

Repeated cyberattacks on critical infrastructure in Ukraine have increased the feeling of vulnerability among the people and engendered an atmosphere of distrust in the Ukrainian government. This feeling of insecurity has been growing since the beginning of the conflict. However, the accelerating rhythm of cyberattacks and their increasing sophistication in the period since January 2017 likely augment the feeling of insecurity. The fact that a tax filing company server was used to spread the NotPetya ransomware may have highlighted to people their own vulnerability, while further eroding trust in Ukrainian companies.

4.2 Economic effects

Economic effects observed since January 2017 were limited to the physical damage caused by the destructive malware and the increasing use of ransomware by state actors.

Damage from malware attacks

Since January 2017, several cyberattacks have rendered computers and machines unusable. The main costs consist of the replacement of damaged computers and machines, and the engagement of cybersecurity firms to ensure the removal of any remaining malware and that vulnerabilities are patched. Unfortunately, it was not possible to find data on the exact costs of the disruptive cyberattacks in Ukraine. It can be assumed that the two attacks on the power grid and the destructive effects of NotPetya caused significant costs to the Ukrainian economy. For example, NotPetya has damaged approximately 17,000 computers around the world and approximately 60% were located in Ukraine (Palmer, 2017). In all likelihood, this represents significant damage to Ukrainian people, and the associated costs with this event may be quite high. Conversely, VPNFilter was uncovered before any damage had been done, but not all infected devices were cleared entirely of the malware. Thus, despite its timely discovery, the malware remains a threat.

Ransomware

State actors employ ransomware attacks with increasing frequency. In 2017, evidence indicated state actors were behind several ransomware attacks. While WannaCry attracted significant media attention, further attacks like NotPetya, XData, PSCrypt and BadRabbit also targeted computers in Ukraine. Other cyberactors, for example North Korea, use ransomware to generate revenue. Interestingly, the tools targeting Ukraine disguised themselves as ransomware but in fact were not intended to incur financial gain. State actors used ransomware to distract and divert attention from their true targets (Borys, 2017; Cimpanu, 2017b, 2017a). Ukraine provides a unique cast study in this regard; in no other instance was ransomware used by an alleged state-actor to directly target computers in one country.

4.3 Technological effects

The technological effects resulting from cyber-activities in the Ukrainian conflict since 2017 are centered on the discovery of new sophisticated malware, and the observation that Ukraine has become a testing ground for malware still in development.

New sophisticated malware

Since January 2017, it would appear that the sophistication of both infection vectors and the malware increased. NotPetya was delivered through a malicious update of a legitimate tax filing software, and stole code from other malware tools to more effectively disguise itself a ransomware. By cloaking itself in the guise of a ransomware, NotPetya's goal was to mislead about its true goal, which was to damage. NotPetya spread throughout Ukraine only a month after the WannaCry ransomware that affected machines worldwide and paralyzed thousands of computers. However, it is unclear if the timeline of NotPetya was coordinated with the spread of WannaCry, or if it was coincidental. Another technological development was the observation of highly sophisticated malware, that targets connected devices, that can survive reboots. This feature indicates that actors behind VPNFilter are persistent and determined to maintain their access to devices (Largent, 2018a). The growing sophistication of cybertools used in Ukraine indicates that attackers targeting Ukrainian institutions are actively learning and developing new skills.

Ukraine as testing ground

Cybersecurity experts have said that Ukraine could have become a prime space for Russia to test cybertools. Experts argue that the cyberattacks on the Ukrainian power grid set a precedent, and indicated that cyberattackers were both willing and able to cripple critical infrastructure if deemed necessary. Both attacks on the Ukrainian power grid only lasted a few hours and targeted only the substations. The attacks could have caused more damage if they had lasted longer or targeted an actual power plant. Cybersecurity experts believe that the attackers limited their aims because the attackers were only testing their tools. In the case of CrashOverride, it is important to specify that it is not the malware itself that caused damage, but that it enabled the attackers to gain access to the ICS and disrupt them (Dragos Inc., 2017; Greenberg, 2017a).

4.4 International effects

The effects of the recent cyberattacks in Ukraine on international relations include the continued restraint showed by conflict parties in not escalating tensions further. Events since January 2017 also highlighted the continued lack of international support for Ukraine to help guard against Russia.

Lot of attention but restraint in cyberattacks

While cyberattacks in Ukraine seem to have intensified and increased since early 2017, they nevertheless remained below a certain threshold that could have caused further escalation in the conflict. The two attacks on the Ukrainian power grid could be considered as high-level cyberattacks given that they targeted critical infrastructure and set a precedent for acceptable targets. However, the attackers restrained themselves to limit damage. In the case of NotPetya, the malware spread outside Ukraine and paralyzed several companies around the world. However, cybersecurity experts assumed that the attackers had underestimated the contagiousness of the malware and did not intend for it to spread outside Ukraine (Cherepanov, 2017a). Since January 2017, no cyberattacks caused an escalation in the conflict or an international intervention. The attackers appeared to know that they were operating in a gray zone between an open conflict and sustained hostilities, and were thus testing “red lines” (Brantly et al., 2017; Greenberg, 2017a). Perpetrators tested how far they can go with cyber operations before their actions caused an international response. Because there are no binding international norms for cyberspace, there are currently no set “red-lines”. However, if “red lines” are found in Ukraine, they might set a precedent that might serve in other international conflicts or even evolve into an international norm. Perpetrators could also be seeking to signal the extent of their cyber capabilities to Western states and warn them that a similar set of events could also happen in their country (Patterson, 2017).

Lack of international support

Because cyberattacks occur in a gray zone between open conflict and sustained hostilities, international support to Ukraine has been limited. International help has mainly consisted of financial contributions for material and educational support. NATO created a Cyber Defense Trust Fund in 2014, but their monetary contributions are limited and only a small number of NATO members participate (Fiscutean, 2015; NATO Trust Fund, 2016). The US provides material support and expertise, but it also is limited (US Embassy Kyiv, 2017). The reality is that Ukraine is geographically too close to Russia and too far from Western states to be able to generate more support. Four years after the annexation of Crimea, the situation in East Ukraine remains more or less the same.

5 Policy consequences

This section suggests general recommendations to mitigate the risks of similar cyberattacks as the ones in Ukraine.

5.1 Fight spear phishing

Both cyberattacks targeting Ukrainian power stations proved that attackers with the dedication and the resources can disrupt critical infrastructure. The malware was sophisticated and the attacks planned well in advance. For the cyberattack of December 2015, the infection vector was spear phishing emails that were sent at least six months before the attack. Therefore, it is necessary to raise awareness and take measures against spear phishing. Critical infrastructure operators could organize sensitization campaigns to raise awareness among their employees. Operators could also encourage employees to report phishing emails and implement standardized procedures in case of infection. Such measures would help operators to identify and deal with an intrusion more rapidly. Technically, critical infrastructure operators could also implement email authentication systems like the Sender Policy Framework (SPF) that authenticate the sender of an email. This would make it easier for employees to identify malicious emails.

5.2 Raise awareness on the cybersecurity of connected devices and implement standards

A recent issue observed in the Ukrainian conflict through the case of VPNFilter was the particular challenge of responding to connected devices that were infected. These devices are difficult to patch and do not have built-in anti-virus software. It is important to raise awareness on the fact that these devices are at risk. States could implement security standards for these devices to reduce the risk of infection. However, zero-day vulnerabilities would still exist. Therefore, manufacturers of these devices could improve the cybersecurity of their products and/or partner with cybersecurity firms to inform users when a specific threat targets their products.

5.3 Monitoring the Ukrainian conflict

NotPetya affected more states than just Ukraine. It is therefore imperative to closely monitor the conflict to be able to detect escalations, and how they might affect outside states, as quickly as possible. States should pay close attention to cyber-activities in Ukraine, as the country appears to have become a testing ground for Russian cybertools still in development.

6 Annex 1

Revised non-exhaustive table of the various cyberattacks occurring during the Ukrainian Euromaidan protests and the conflict with Russia.

Rows in light blue are new cyberattacks that were not included in the Hotspot Analysis on Cyber and Information warfare in the Ukrainian conflict.

G = Government institutions, M = Media outlets, IO = Intergovernmental Organization, O = Others

Date	Victim	Type of victim	Alleged perpetrator	Technique/Tool
07.11.2013	CCDOE website	IO	CyberBerkut or Anonymous Ukraine	DDoS (Carr, 2014)
15.11.2013	Ukraine Customs Services	G	Anonymous	Unspecified data breach (Kovacs, 2013a)
24-25.11.2013	Newspaper Ukraiska Pravda website	M	Pro-Russian actor	DDoS (Ukraine investigations, 2014)
26.11.2013	TV channel Hromadske website	M	Pro-Russian actor	DDoS (Ukraine investigations, 2014)
26.11.2013	News website censor.net	M	Pro-Russian actor	Wiped all information on the website (Ukraine investigations, 2014)
31.11.2013	Ukrainian Ministry of Internal Affairs website	G	Protesters of the Euromaidan movement	DDoS (Ukraine investigations, 2014)
04.12.2013	Pro-Russian news website of Ukrainskaya Pravda	M	Pro-Ukrainian actor	DDoS (Ukraine investigations, 2014)
10.12.2013	Ukraine Brovary region website	G	Anonymous affiliated group called Clash Hackerz	Unspecified data breach and defacement (Kovacs, 2013b)
28.12.2013	Emails from the Ukrainian Volyn regional state administration website	G	Anonymous	Credentials and passwords for email accounts obtained by a phishing campaign (Johnstone, 2013)
07.01.2014	Ukrainian TV 5 Channel News website	M	Pro-Russian actor	DDoS (Ukraine investigations, 2014)
09.01.2014	The webpage maidan.ua.org	O	Pro-Russian actor	DDoS (Ukraine investigations, 2014)
16.01.2014	Website of the Greek-Catholic Church in Ukraine	O	Pro-Russian actor	DDoS (Ukraine investigations, 2014)
28.01.2016	Ukrainian TV channel website espresso.tv	M	Pro-Russian actor	DDoS (Ukraine investigations, 2014)
31.01.2014	30 Ukrainian government and media websites	G/M	Ukrainian neo-fascist party Svoboda	Defacement (Waqas, 2014)
11.02.2014	A regional office of the Ukrainian Democratic Alliance for Reform party	O	Anonymous	Unspecified data breach (Johnstone, 2014)

Date	Victim	Type of victim	Alleged perpetrator	Technique/Tool
18.02.2014	Ukrainian members of Parliament's cell phones	G	Unknown	Cell phones flooded by SMS to prevent members of Parliament from using their phones (Weedon, 2015)
27-28.02.2014	Ukrtelecom infrastructures in Crimea raided	O/G	Armed "little-green-men" (presumed Russian special forces troops)	Cutting cables (Martin-Vegue, 2015)
03.2014	Ukrainian government's website	G	Unknown	Shut down for 72 hours (Weedon, 2015)
03.2014	Ukrainian media outlets' websites	M	Unknown	DDoS (Weedon, 2015)
03.2014	Ukrainian government's network	G	Unknown	Snake malware (Sanger and Erlanger, 2014)
02.03.2014	Pro-Russian news website RT.com	M	Unknown	Defacement, replacing certain words by "Nazi" (Perlroth, 2014)
04.03.2014	Ruptly (a video website part of RT)	M	Unknown	DDoS (Kovacs, 2014)
07.03.2014	The Kremlin's website	G	Cyber Hundred or Null Sector or another pro-Ukrainian actor	DDoS (Maurer, 2015)
14.03.2014	Russian President's website and Bank of Russia's websites	G	Cyber Hundred or Null Sector or another pro-Ukrainian actor	DDoS (Ukraine investigations, 2014)
14.03.2014	Russian news portal lenta.ru	M	Cyber Hundred or Null Sector or another pro-Ukrainian actor	DDoS (Ukraine investigations, 2014)
16.03.2014	Several NATO websites	IO	CyberBerkut	DDoS (Bejtlich, 2015)
18.03.2014	Regional TV of Rivne in Western Ukraine	M	CyberBerkut	DDoS (Ukraine investigations, 2014)
18.03.2014	Ukrainian news portal zik.ua	M	Pro-Russian actor	DDoS (Ukraine investigations, 2014)
24.03.2014	7 million credit cards	O	Anonymous	Data breach and leak (Passeri, 2014a)
03.04.2014	Website of the Coordination Council of Sevastopol	G	Pro-Ukrainian actor	Defacement and rerouting (Ukraine investigations, 2014)
04.04.2014	Websites of Ukrainian Main Prosecutor Office and of Ukrainian Ministry of internal Affairs	G	CyberBerkut	DDoS (Ukraine investigations, 2014)
09.04.2014	Ukrainian Main Prosecutor's Office's webpage	G	CyberBerkut or another pro-Russian actor	DDoS (Ukraine investigations, 2014)
09.04.2014	Ukrainian blog RoadNews	M	Pro-Russian actor	DDoS (Ukraine investigations, 2014)
10.04.2014	The Russian Lower Parliament Chamber's (Duma) website	G	Pro-Ukrainian actor	DDoS (Ukraine investigations, 2014)
05.2014	Ukrainian Privatbank	O	CyberBerkut	Data theft (The Moscow Times, 2014)

Date	Victim	Type of victim	Alleged perpetrator	Technique/Tool
25.05.2014	Ukrainian Central Election Commission's website	G	CyberBerkut	Defacement and unspecified malware (Koval, 2015; Weedon, 2015)
26.07.2014	Email of the Ukrainian Colonel Pushenko	G	CyberBerkut	Data breach and leak (Passeri, 2014b)
09.08.2014	Regional department of the law enforcement in Dnepropetrovsk, Ukraine	G	CyberBerkut	Data breach and leak (Passeri, 2014c)
10.2014	Ukrainian Central Election Commission's website	G	Unknown	DDoS (Martin-Vegue, 2015)
24.10.2014	City billboard in Kiev	G/O	CyberBerkut	Depiction of Ukrainian members of Parliament as war criminals (Lange-Ionatamishvili and Svetoka, 2015)
20-21.11.2014	Several Ukrainian governmental websites	G	CyberBerkut	Defacement of the websites with a message on Joe Biden being a fascist (Shevchenko, 2014)
2015	Bellingcat	O	APT28	Spear phishing campaign (Ashok, 2016)
02.01.2015	Ukrainian law enforcement and justice organizations	G	Anonymous	Data breach and leak (Passeri, 2015a)
27.02.2015	US private military contractor involved in Ukraine, Green Group Defense Service	O	CyberBerkut	Access to information on phones (Passeri, 2015b)
25.04.2015	Ukrainian government network	G	Unknown	Operation Armageddon malware (Bejtlich, 2015)
04-05.2015	Ukrainian Ministry of Defense	G	Unknown	Targeted intrusions into the network (Crowdstrike, 2016, p. 5)
18.08.2015	Several Ukrainian websites	O	CyberBerkut	DDoS (Passeri, 2015c)
10.2015	StarLightMedia (Ukrainian media outlet)	M	Allegedly Sandworm	BlackEnergy malware (Greenberg, 2017a)
13.10.2015	The Dutch Safety Board (investigative body for the crash of flight MH17)	O	Allegedly APT28	Spear phishing and another unspecified type of cyberattack (Foxall, 2016)
23.12.2015	Ukrainian power grid	O/G	Unknown (probably Russian group)	BlackEnergy3 malware (Zetter, 2016)
01.2016	Kiev Boryspil Airport	O/G	Unknown (probably Russian group)	Similar to the malware from the power grid, probably BlackEnergy3 (Bolton, 2016; Polityuk and Prentice, 2016)
02.2016	Bellingcat website and email from a Bellingcat journalist	O	CyberBerkut	Defacement and leak of document stolen from the journalist's email account (Ashok, 2016; Crowdstrike, 2016, p. 5)
06.05.2016	Emails of Boris Dobrodeev, former boss of the Russian social network, vKontakte	O	Anonymous	Data breach and leak (Passeri, 2016)
05.2016	Alleged pro-Russian Ukrainian journalists	M	Myrotvorets a Ukrainian nationalist hacker group	Data breach and leak (Cimpanu, 2016)
06-12.2016	Ukrainian financial institutions	O	Sandworm	Cyberespionage with Python/TeleBot Trojan (Cherepanov, 2016)

Date	Victim	Type of victim	Alleged perpetrator	Technique/Tool
07.2016	20 Russian organizations (governmental, scientific and defense institutions)	G	Unknown	Unspecified malware (BBC News, 2016a)
07.2016	Ukrainian artillery	G	APT28	Malicious application for Android and Apple smartphones that intercepts communications and gives away user locations (Crowdstrike, 2016).
24.08.2016	Ukrainian Ministry of Defense and Ukrainian National Guard's Twitter and Instagram accounts	G	Pro-Russian or Russian actor named SPRUT	Defacement of their Twitter and Instagram accounts (Starks, 2016).
08.2016	Alleged pro-Russian Ukrainian journalists	M	Myrotvorets a Ukrainian nationalist hacker group	Data breach and leak (Cimpanu, 2016)
25.10.2016	Surkov's emails	G	CyberHunta	"Special software" (Miller, 2016)
11.2016	OSCE	IO	Allegedly APT28	Unspecified (BBC News, 2016b)
06-08.12.2016	Ukrainian Ministry of Finance	G	Unknown	DDoS attack simultaneous with a system breach (Zetter, 2017).
06-08.12.2016	Ukrainian State Treasury	G	Unknown	DDoS attack simultaneous with a system breach (Zetter, 2017)
13.12.2016	Ukraine Ministry of Defense	G	Unknown	DDoS (Reuters, 2016)
14.12.2016	Ukrainian State Administration of Railway Transport	G	Unknown	DDoS attack simultaneous with a system breach (Zetter, 2017)
17.12.2016	Ukrainian power substation in Pivnichna near Kiev	O/G	Unknown	BlackEnergy3 malware (Goodin, 2017)
03.2017	Ukrainian computers	O	Sandworm	Ransomware, an early version of NotPetya (Cherepanov, 2017c)
16.05.2017	Ukrainian president Poroshenko's official website	G	Unknown	Unknown type of cyberattack that caused the unavailability of the website for a few hours (BBC News, 2017a)
18.05.2017	Ukrainian computers	O	Sandworm	Xdata Ransomware, an early version of NotPetya (Cherepanov, 2017c)
21.06.2017	Ukrainian computers	O	Highly likely to be Sandworm	PSCrypt ransomware (Cimpanu, 2017b)
26.06.2017	Ukrainian computers	O	Highly likely to be Sandworm	Ransomware that visually looks like WannaCry (Cimpanu, 2017a)
27.06.2017	Ukrainian infrastructures, primarily computers, before spreading to the rest of the world	G/O	Sandworm	NotPetya malware was disguised as ransomware but was designed to cause damage (Cherepanov, 2017a)
10.08.2017	Ukrainian postal service website	G	Unknown	DDoS attack (BBC News, 2017d)
24.10.2017	Ukrainian and Russian computers	O	Allegedly APT28	BadRabbit ransomware (Bing, 2017)
23.05.2018	Routers worldwide, though primarily affecting Ukrainian targets	O	APT28	VPNFilter malware (Largent, 2018a, 2018b)

7 Glossary

Advanced Persistent Threat (APT): a targeted threat that tries to gain access to a computer system. Once inside a network, it remains hidden and is usually difficult to remove when discovered (Command Five Pty Ltd, 2011; DellSecureWorks, 2014).

Backdoor: Part of a software code that allows hackers to remotely access a computer without the user's knowledge (Ghernaouti-Hélie, 2013, p. 426).

Botnet: Network of infected computers which can be accessed remotely and controlled centrally in order to launch coordinated attacks (Ghernaouti-Hélie, 2013, p. 427).

Data breach: Event in which information of a sensitive nature is stolen from a network without the users' knowledge (TrendMicro, 2017).

Distributed Denial of Service (DDoS): Act of overwhelming a system with a large number of packets through the simultaneous use of infected computers (Ghernaouti-Hélie, 2013, p. 431).

Domain Name: The alphabetic identifier of a website attached to its unique Internet Protocol address (Internet Corporation For Assigned Names and Numbers, 2016).

Euromaidan movement: Literally "European Square"; a protest movement in support of the European Union Association Treaty that was cancelled by former Ukrainian President Yanukovych (Chervonenko, 2013).

False-flag: act of deceiving an adversary into thinking that the cyberattack was perpetrated by someone else (Pihelgas, 2015).

Hacktivism: use of hacking techniques for political or social activism (Ghernaouti-Hélie, 2013, p. 433).

Firmware: A software program programmed on a hardware device providing the instructions for communication between the device and other hardware. Firmware is stored in the flash read-only memory of the device (TechTerms, 2016).

Malware: Malicious software that can take the form of a virus, a worm or a Trojan horse (Collins and McCombie, 2012).

Man-in-the-middle-attack (MiM/MitM/MitMA): When an attacker is able to intercept and modify a message at will without the sender and receiver's knowledge (Ghernaouti-Hélie, 2013, p. 436).

Patch: Software update that repairs one or several identified vulnerabilities (Ghernaouti-Hélie, 2013, p. 437).

Patriotic hacking: Sometimes also referred to as nationalistic hacking. A group of individuals originating from a specific state engage in cyberattacks in defense against actors that they perceive to be enemies of their country (Denning, 2011, p. 178).

Ransomware: Malware that locks the user's computer system and only unlocks it when a ransom is paid (Trend Micro, 2017).

Sender Policy Framework (SPF): Technical system validating email senders as originating from an authenticated connection in order to prevent email spoofing (Openspf, 2010).

Spear phishing: A sophisticated phishing technique that not only imitates legitimate webpages, but also selects potential targets and adapts malicious emails to them. Emails often look like they come from a colleague or a legitimate company (Ghernaouti-Hélie, 2013, p. 440).

Trojan horse: Malware hidden in a legitimate program in order to infect and hijack a system (Ghernaouti-Hélie, 2013, p. 441).

Virtual Private Network (VPN): Private network within a public network that uses encryption to remain private (PCmag, 2016).

Website defacement: Cyberattack replacing website pages or elements with other pages or elements (Ghernaouti-Hélie, 2013, p. 442).

Wiper: Feature that completely erases data from a hard disk (Novetta, 2016, p. 57).

Worm: Standalone, self-replicating program infecting and spreading to other computers through networks (Collins and McCombie, 2012, p. 81).

Zero-day exploit / vulnerabilities: Security vulnerabilities of which software developers are not aware and which can be used to hack a system (Karnouskos, 2011).

8 Abbreviations

APT	Advanced Persistent Threat
C&C	Command and Control Infrastructure
DDoS	Distributed Denial of Service
FBI	US Federal Bureau of Investigation
FSB	Federal Security Service of the Russian Federation
GRU	Main Intelligence Directorate - Russia
ICS	Industrial Control System
NAS	Network-Attached Storage
NATO	North Atlantic Treaty Organization
OSCE	Organization for Security and Co-operation in Europe
SBU	Ukraine Security Services
SPF	Sender Policy Framework
VPN	Virtual Private Network

9 Bibliography

Ashok, I., 2016. Journalists investigating MH17 hacked by Russia-backed Fancy Bear hackers - ThreatConnect [WWW Document]. Int. Bus. Times. URL http://www.ibtimes.co.uk/journalists-investigating-mh17-hacked-by-russia-backed-fancy-bear-hackers-threatconnect-1583881 (accessed 08.02.17).

BBC News, 2017a. Ukraine president's site "attacked by Russia" [WWW Document]. BBC News. URL https://www.bbc.com/news/world-europe-39944158 (accessed 13.06.18).

BBC News, 2017b. Ukraine wants membership plan talks, says Poroshenko [WWW Document]. BBC News. URL https://www.bbc.com/news/world-europe-40557477 (accessed 14.06.18).

BBC News, 2017c. "Bad Rabbit" ransomware strikes Ukraine and Russia [WWW Document]. BBC News. URL https://www.bbc.com/news/technology-41740768 (accessed 13.06.18).

BBC News, 2017d. Ukrainian postal service hit by 48-hour cyber-attack [WWW Document]. BBC News. URL https://www.bbc.com/news/technology-40886418 (accessed 13.06.18).

BBC News, 2016a. Russia cyber attack: Large hack "hits government" [WWW Document]. BBC News. URL http://www.bbc.com/news/world-europe-36933239 (accessed 31.10.16).

BBC News, 2016b. OSCE security monitors targeted by hackers [WWW Document]. BBC News. URL http://www.bbc.com/news/world-europe-38451064 (accessed 05.01.17).

Bejtlich, R., 2015. Strategic Defence in Cyberspace: Beyond Tools and Tactics, in: Cyber War in Perspective: Russian Aggression against Ukraine. Kenneth Geers, Tallinn, pp. 159–170.

Bennetts, M., 2017. Ukraine and separatists begin largest prisoner exchange of conflict [WWW Document]. The Guardian. URL https://www.theguardian.com/world/2017/dec/27/ukraine-and-separatists-begin-largest-prisoner-exchange-of-conflict (accessed 14.06.18).

Bing, C., 2018a. Russian-linked VPNFilter malware is even worse than originally thought, new research suggests [WWW Document]. Cyberscoop. URL https://www.cyberscoop.com/russian-linked-vpnfilter-malware-even-worse-originally-thought-new-research-suggests/ (accessed 19.06.18).

Bing, C., 2018b. Researchers uncover sophisticated botnet aimed at possible attack inside Ukraine [WWW Document]. Cyberscoop. URL https://www.cyberscoop.com/vpnfilter-ukraine-talos-cyber-threat-alliance/ (accessed 18.06.18).

Bing, C., 2017. Ukraine blames infamous Russian hackers for “BadRabbit” ransomware attack [WWW Document]. Cyberscoop. URL https://www.cyberscoop.com/fancy-bear-bad-rabbit-ransomware-security-service-of-ukraine/ (accessed 03.06.18).

Bolton, D., 2016. Ukraine says major cyberattack on Kiev’s Boryspil airport was launched from Russia [WWW Document]. Independent. URL http://www.independent.co.uk/news/world/europe/ukraine-cyberattack-boryspil-airport-kiev-russia-hack-a6818991.html (accessed 19.01.17).

Borys, C., 2017. Ukraine braces for further cyber-attacks [WWW Document]. BBC News. URL https://www.bbc.com/news/technology-40706093 (accessed 13.06.18).

Brantly, A.F., Cal, N.M., Winkelstein, D.P., 2017. DEFENDING THE BORDERLAND Ukrainian Military Experiences with IO, Cyber, and EW.

Carr, J., 2014. Rival hackers fighting proxy war over Crimea [WWW Document]. CNN. URL http://edition.cnn.com/2014/03/25/opinion/crimea-cyber-war/ (accessed 18.11.16).

Cherepanov, A., 2017a. TeleBots are back: Supply-chain attacks against Ukraine [WWW Document]. Welivesecurity ESET. URL https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine/ (accessed 14.06.18).

Cherepanov, A., 2017b. WIN32/INDUSTROYER A new threat for industrial control systems. ESET LLC.

Cherepanov, A., 2017c. Analysis of TeleBots’ cunning backdoor [WWW Document]. Welivesecurity ESET. URL https://www.welivesecurity.com/2017/07/04/analysis-of-telebots-cunning-backdoor/ (accessed 13.06.18).

Cherepanov, A., 2016. The rise of TeleBots: Analyzing disruptive KillDisk attacks [WWW Document]. ESET. URL http://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks/ (accessed 20.01.17).

Chervonenko, V., 2013. Ukraine’s EU options “still open” [WWW Document]. BBC News. URL http://www.bbc.com/news/world-europe-25087160 (accessed 06.12.16).

Cimpanu, C., 2017a. Ransomware Attacks Continue in Ukraine with Mysterious WannaCry Clone [WWW Document]. BleepinComputer. URL https://www.bleepingcomputer.com/news/security/ransomware-attacks-continue-in-ukraine-with-mysterious-wannacry-clone/ (accessed 28.06.18).

Cimpanu, C., 2017b. Before NotPetya, There Was Another Ransomware That Targeted Ukraine Last Week [WWW Document]. BleepinComputer. URL https://www.bleepingcomputer.com/news/security/before-notpetya-there-was-another-ransomware-that-targeted-ukraine-last-week/ (accessed 27.06.18).

Cimpanu, C., 2017c. XData Ransomware on a Rampage in Ukraine [WWW Document]. BleepinComputer. URL https://www.bleepingcomputer.com/news/security/xdata-ransomware-on-a-rampage-in-ukraine/ (accessed 28.06.18).

Cimpanu, C., 2016. Pro-Ukraine Hackers Leak Personal Details of Ukrainian and Foreign Journalists [WWW Document]. Softpedia. URL http://news.softpedia.com/news/pro-ukraine-hackers-leak-personal-details-of-ukrainian-and-foreign-journalists-507926.shtml (accessed 28.03.17).

Collins, S., McCombie, S., 2012. Stuxnet: the emergence of a new cyber weapon and its implications. J. Polic. Intell. Count. Terror. 7, 80–91. https://doi.org/10.1080/18335330.2012.653198

Command Five Pty Ltd, 2011. Advanced Persistent Threats: A Decade in Review.

Crowdstrike, 2016. Use of Fancy Bear Android malware in tracking of Ukrainian field artillery units.

DellSecureWorks, 2014. Advanced Threat Protection with Dell SecureWorks Security Services. Dell Inc.

Denning, D.E., 2011. Cyber Conflict as an Emergent Social Phenomenon, in: Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications. Holt and Schell, pp. 170–186.

Dragos Inc., 2017. Crash Override Analysis of the Threat to Electric Grid Operations. Dragos Inc.

Fiscutean, A., 2015. Cyber war in Ukraine: How NATO is helping the country defend itself against digital threats [WWW Document]. ZDNet Eur. URL http://www.zdnet.com/article/ukraines-cyber-warfare-how-nato-helps-the-country-defend-itself-against-digital-threats/ (accessed 17.11.16).

Foxall, A., 2016. Putin’s Cyberwar: Russia’s Statecraft in the Fifth Domain.

F-Secure, 2014. BLACKENERGY & QUEDAGH The convergence of crimeware and APT attacks. F-Secure, Helsinki.

Geller, E., 2018. White House blames Russia for massive Ukraine cyberattack [WWW Document]. POLITICO. URL https://www.politico.com/story/2018/02/15/

white-house-blames-russia-for-massive-ukraine-cyberattack-638151 (accessed 28.06.18).

Ghernaouti-Hélie, S., 2013. Cyberpower: crime, conflict and security in cyberspace, 1. ed. ed, Forensic sciences. EPFL Press, Lausanne.

Goodin, D., 2017. Hackers trigger yet another power outage in Ukraine [WWW Document]. Ars Tech. URL http://arstechnica.com/security/2017/01/the-new-normal-yet-another-hacker-caused-power-outage-hits-ukraine/ (accessed 19.01.17).

Greenberg, A., 2017a. How an Entire Nation Became Russia's Test Lab For Cyberwar [WWW Document]. WIRED. URL https://www.wired.com/story/russian-hackers-attack-ukraine/ (accessed 26.06.18).

Greenberg, A., 2017b. Your Guide to Russia's Infrastructure Hacking Teams [WWW Document]. WIRED. URL https://www.wired.com/story/russian-hacking-teams-infrastructure/ (accessed 13.06.18).

Hern, A., 2017a. Bad Rabbit: Game of Thrones-referencing ransomware hits Europe [WWW Document]. The Guardian. URL https://www.theguardian.com/technology/2017/oct/25/bad-rabbit-game-of-thrones-ransomware-europe-notpetya-bitcoin-decryption-key (accessed 14.06.18).

Hern, A., 2017b. WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017 [WWW Document]. The Guardian. URL https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware (accessed 29.06.18).

Internet Corporation For Assigned Names and Numbers, 2016. Glossary [WWW Document]. ICANN. URL https://www.icann.org/resources/pages/glossary-2014-02-03-en#i (accessed 04.11.16).

Johnstone, L., 2014. #OpIndependence. Vitali Klitschko's UDAR party hacked. Confidential data leaked [WWW Document]. Cyberwarnews. URL https://www.cyberwarnews.info/2014/02/14/opindependence-vitali-klitschkos-udar-party-hacked-confidential-data-leaked/ (accessed 20.01.17).

Johnstone, L., 2013. Anonymous leak Ukraine Government Emails And Credentials for #OpUkraine [WWW Document]. Cyberwarnews. URL https://www.cyberwarnews.info/2013/12/28/anonymous-leak-ukraine-government-emails-and-credentials-for-opukraine/ (accessed 20.01.17).

Karnouskos, S., 2011. Stuxnet worm impact on industrial cyber-physical system security. IEEE, pp. 4490–4494. https://doi.org/10.1109/IECON.2011.6120048

Kasza, A., Reichel, D., 2017. The Gamaredon Group Toolset Evolution [WWW Document]. Paloalto Netw. URL https://researchcenter.paloaltonetworks.com/2017/02/unit-42-title-gamaredon-group-toolset-evolution/ (accessed 29.06.18).

Kovacs, E., 2014. Website of International Video News Agency Ruptly Hit With DDOS Attack [WWW Document]. Softpedia. URL http://news.softpedia.com/news/Website-of-International-Video-News-Agency-Ruptly-Hit-With-DDOS-Attack-430390.shtml (accessed 20.01.17).

Kovacs, E., 2013a. Ukraine's State Customs Service Targeted by Anonymous Hackers [WWW Document]. Softpedia. URL http://news.softpedia.com/news/Ukraine-s-State-Customs-Service-Targeted-by-Anonymous-Hackers-400518.shtml (accessed 20.01.17).

Kovacs, E., 2013b. Government Website of Ukraine's Brovary Region Hacked [WWW Document]. Softpedia. URL http://news.softpedia.com/news/Government-Website-of-Ukraine-s-Brovary-Region-Hacked-407646.shtml (accessed 20.01.17).

Koval, N., 2015. Revolution Hacking, in: Cyber War in Perspective: Russian Aggression against Ukraine. Kenneth Geers, Tallinn, pp. 55–58.

Lange-Ionatamishvili, E., Svetoka, S., 2015. Strategic Communications and Social Media in the Russia Ukraine Conflict, in: Cyber War in Perspective: Russian Aggression against Ukraine. Kenneth Geers, Tallinn, pp. 103–112.

Largent, W., 2018a. New VPNFilter malware targets at least 500K networking devices worldwide [WWW Document]. Talos. URL https://blog.talosintelligence.com/2018/05/VPNFilter.html (accessed 19.06.18).

Largent, W., 2018b. VPNFilter Update - VPNFilter exploits endpoints, targets new devices [WWW Document]. Talos. URL https://blog.talosintelligence.com/2018/06/vpnfilter-update.html (accessed 19.06.18).

Luhn, A., 2017. Ukraine blocks popular social networks as part of sanctions on Russia [WWW Document]. The Guardian. URL https://www.theguardian.com/world/2017/may/16/ukraine-blocks-popular-russian-websites-kremlin-role-war (accessed 13.06.18).

Lyngaas, S., 2018. State Department to double cyberdefense aid to Ukraine [WWW Document]. Cyberscoop. URL https://www.cyberscoop.com/state-department-ukraine-cyber-aid/ (accessed 14.06.18).

Mamedov, O., Sinitsyn, F., Ivanov, A., 2017. Bad Rabbit ransomware [WWW Document]. Securelist. URL https://securelist.com/bad-rabbit-ransomware/82851/ (accessed 28.06.18).

Marcus, J., 2017. Zapad: What can we learn from Russia's latest military exercise? [WWW Document]. BBC News. URL https://www.bbc.com/news/world-europe-41309290 (accessed 13.06.18).

Martin-Vegue, T., 2015. Are we witnessing a cyber war between Russia and Ukraine? Don't blink - you might miss it [WWW Document]. CSOonline.com. URL http://www.csoonline.com/article/2913743/cyber-attacks-espionage/are-we-witnessing-a-cyber-war-between-russia-and-ukraine-dont-blink-you-might-miss-it.html (accessed 17.11.16).

Maurer, T., 2015. Cyber Proxies and the Crisis in Ukraine, in: Cyber War in Perspective: Russian Aggression against Ukraine. Kenneth Geers, Tallinn, pp. 79–86.

Miller, C., 2016. Inside The Ukrainian "Hacktivist" Network Cyberbattling The Kremlin [WWW Document]. RadioFreeEurope RadioLiberty. URL http://www.rferl.org/a/ukraine-hacktivist-network-cyberwar-on-kremlin/28091216.html (accessed 03.11.16).

Nakashima, E., 2018. Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes [WWW Document]. Wash. Post. URL https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html?utm_term=.711e6198c53b (accessed 14.06.18).

NATO Trust Fund, 2016. Ukraine Cyber Defence.

Novetta, 2016. Operation Blockbuster: Unraveling the long thread of the Sony attack. Novetta, McLean,Virginia, USA.

Openspf, 2010. Sender Policy Framework [WWW Document]. Send. Policy Framew. URL http://www.openspf.org/Introduction (accessed 03.01.17).

Otto, G., 2018. FBI shuts down domain behind Russian "VPNFilter" botnet [WWW Document]. Cyberscoop. URL https://www.cyberscoop.com/vpnfilter-botnet-fbi-seizure-apt-28-fancy-bear/ (accessed 18.06.18).

Paganini, P., 2017a. Following NotPetya NATO Increases Support for Ukraine's Cyber Defenses [WWW Document]. Secur. Aff. URL http://securityaffairs.co/wordpress/60941/cyber-warfare-2/nato-support-ukraine-cybersecurity.html (accessed 14.06.18).

Paganini, P., 2017b. The Gamaredon Group is back with new weapons in its arsenal [WWW Document]. Secur. Aff. URL http://securityaffairs.co/wordpress/56756/intelligence/gamaredon-group-backdoor.html (accessed 28.06.18).

Palmer, D., 2017. Petya ransomware attack: How many victims are there really? [WWW Document]. ZDNet Eur. URL https://www.zdnet.com/article/petya-ransomware-attack-how-many-victims-are-there-really/ (accessed 29.06.18).

Passeri, P., 2016. 1-15 May 2016 Cyber Attacks Timeline [WWW Document]. HACKMAGEDDON. URL http://www.hackmageddon.com/2016/06/08/1-15-may-2016-cyber-attacks-timeline/ (accessed 28.03.17).

Passeri, P., 2015a. 1-15 January 2015 Cyber Attacks Timeline [WWW Document]. HACKMAGEDDON. URL http://www.hackmageddon.com/2015/01/20/1-15-january-2015-cyber-attacks-timeline/ (accessed 28.03.17).

Passeri, P., 2015b. 16-28 February 2015 Cyber Attacks Timeline [WWW Document]. HACKMAGEDDON. URL http://www.hackmageddon.com/2015/03/01/16-28-february-2015-cyber-attacks-timeline/ (accessed 28.03.17).

Passeri, P., 2015c. 16-31 August 2015 Cyber Attacks Timeline [WWW Document]. HACKMAGEDDON. URL http://www.hackmageddon.com/2015/09/07/16-31-august-2015-cyber-attacks-timeline/ (accessed 28.03.17).

Passeri, P., 2014a. 16-31 March 2014 Cyber Attacks Timeline [WWW Document]. HACKMAGEDDON. URL http://www.hackmageddon.com/2014/04/14/16-31-march-2014-cyber-attacks-timeline/ (accessed 28.03.17).

Passeri, P., 2014b. 16-31 July 2014 Cyber Attacks Timeline [WWW Document]. HACKMAGEDDON. URL http://www.hackmageddon.com/2014/08/05/16-31-july-2014-cyber-attacks-timeline/ (accessed 28.03.17).

Passeri, P., 2014c. 1-15 August 2014 Cyber Attacks Timeline [WWW Document]. HACKMAGEDDON. URL http://www.hackmageddon.com/2014/08/19/1-15-august-2014-cyber-attacks-timeline/ (accessed 28.03.17).

Patterson, D., 2017. Ukraine is a test bed for global cyberattacks that will target major infrastructure [WWW Document]. TechRepublic. URL https://www.techrepublic.com/article/ukraine-is-a-test-bed-for-global-cyberattacks-that-will-target-major-infrastructure/ (accessed 26.06.18).

PCmag, 2016. Definition of: virtual private network [WWW Document]. PCmag. URL http://www.pcmag.com/encyclopedia/term/53942/virtual-private-network (accessed 25.04.17).

Perlroth, N., 2014. Cyberattacks Rise as Ukraine Crisis Spills to Internet [WWW Document]. N. Y. Times. URL http://bits.blogs.nytimes.com/2014/03/04/cyberattacks-rise-as-ukraine-crisis-spills-on-the-internet/ (accessed 18.11.16).

Pihelgas, M., 2015. Mitigating Risks arising from False-Flag and No-Flag Cyber Attacks. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn.

Polityuk, P., 2018. Exclusive: Ukraine says Russian hackers preparing massive strike [WWW Document]. Reuters. URL https://www.reuters.com/article/us-ukraine-cyber-exclusive/exclusive-ukraine-says-russia-hackers-laying-groundwork-for-massive-strike-idUSKBN1JM225 (accessed 28.06.18).

Polityuk, P., Prentice, A., 2016. Ukraine says to review cyber defenses after airport targeted from Russia [WWW Document]. Reuters. URL http://www.reuters.com/article/us-ukraine-cybersecurity-malware-idUSKCN0UW0R0 (accessed 19.01.17).

Reuters, 2016. Ukraine's defence ministry says website hit by cyber attack [WWW Document]. Reuters. URL http://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN1421YT (accessed 24.01.17).

Reuters Staff, 2018. Ukraine power distributor plans cyber defense system for $20 million [WWW Document]. Reuters. URL https://www.reuters.com/article/us-ukraine-cyber-ukrenergo/ukraine-power-distributor-plans-cyber-defense-system-for-20-million-idUSKBN1FQ1TD (accessed 14.06.18).

Sanger, D.E., Erlanger, S., 2014. Suspicion Falls on Russia as 'Snake' Cyberattacks Target Ukraine's Government [WWW Document]. N. Y. Times. URL http://www.nytimes.com/2014/03/09/world/europe/suspicion-falls-on-russia-as-snake-cyberattacks-target-ukraines-government.html?_r=1 (accessed 18.11.16).

Shevchenko, V., 2014. Ukraine conflict: Hackers take sides in virtual war [WWW Document]. BBC News. URL http://www.bbc.com/news/world-europe-30453069 (accessed 28.11.16).

Starks, T., 2016. Russia's cyberspace footprint gets bigger [WWW Document]. PoliticoMagazine. URL http://www.politico.com/tipsheets/morning-cybersecurity/2016/08/russias-cyberspace-footprint-gets-bigger-216075 (accessed 08.02.17).

Symantec Security Response, 2018. VPNFilter: New Router Malware with Destructive Capabilities [WWW Document]. Symantec. URL https://www.symantec.com/blogs/threat-intelligence/vpnfilter-iot-malware (accessed 18.06.18).

TechTerms, 2016. Firmware [WWW Document]. TechTerms. URL http://techterms.com/definition/firmware (accessed 08.12.16).

The Moscow Times, 2014. "Cyber Berkut" Hackers Target Major Ukrainian Bank [WWW Document]. Mosc. Times. URL https://themoscowtimes.com/articles/cyber-berkut-hackers-target-major-ukrainian-bank-37033 (accessed 22.11.16).

Trend Micro, 2017. Ransomware [WWW Document]. Trend Micro. URL https://www.trendmicro.com/vinfo/us/security/definition/ransomware (accessed 19.02.18).

TrendMicro, 2017. Definition [WWW Document]. TrendMicro. URL http://www.trendmicro.com/vinfo/us/security/definition/data-breach (accessed 17.01.17).

Ukraine investigations, 2014. Cyber Wars: The Invisible Front [WWW Document]. Ukr. Investig. URL http://ukraineinvestigation.com/cyber-wars-invisible-front/ (accessed 17.11.16).

US Embassy Kyiv, 2017. Embassy Statement on the First US-Ukraine Bilateral Cyber Dialogue [WWW Document]. US Embassy Ukr. URL https://ua.usembassy.gov/embassy-statement-first-us-ukraine-bilateral-cyber-dialogue/ (accessed 14.06.18).

Walker, S., Borger, J., 2017. US broadens Russia sanctions as Ukraine president visits Trump [WWW Document]. The Guardian. URL https://www.theguardian.com/us-news/2017/jun/20/us-russia-sanctions-ukraine-president-visit (accessed 13.06.18).

Waqas, A., 2014. 30 Ukrainian government and media websites defaced by neo-fascist Svoboda party [WWW Document]. HackRead. URL https://www.hackread.com/ukrainian-government-websites-hacked-by-new-nazi-hackers/ (accessed 20.01.17).

Weedon, J., 2015. Beyond ‘Cyber War’: Russia’s Use of Strategic Cyber Espionage and Information Operations in Ukraine, in: Cyber War in Perspective: Russian Aggression against Ukraine. Kenneth Geers, Tallinn, pp. 67–77.

Zetter, K., 2017. The Ukrainian Power Grid Was Hacked Again [WWW Document]. Motherboard. URL http://motherboard.vice.com/read/ukrainian-power-station-hacking-december-2016-report (accessed 19.01.17).

Zetter, K., 2016. Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid [WWW Document]. Wired. URL https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ (accessed 23.11.16).

CSS
ETH Zurich

The **Center for Security Studies (CSS) at ETH Zurich** is a center of competence for Swiss and international security policy. It offers security policy expertise in research, teaching and consulting. The CSS promotes understanding of security policy challenges as a contribution to a more peaceful world. Its work is independent, practice-relevant, and based on a sound academic footing.